Norton 360™ 6.0

Product Manual

Care for our Environment; 'It's the right thing to do.'
Symantec has removed the cover from this manual to reduce the Environmental Footprint of our products. This manual is made from recycled materials.

Norton 360™ Product Manual

Symantec Corporation
350 Ellis Street,
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1 Getting Started 7
About Norton 360 7
Activation protects you 20
About your Norton Account 24
About Norton Community Watch 32
About Norton Bootable Recovery Tool 34
About updating Norton 360 38
About Network Proxy Settings 48
About Norton 360 status 52

Chapter 2 Monitoring your system's performance 59
About System Insight 59

Chapter 3 Maintaining total protection 103
About total protection 103
About keeping your computer secure 104
About solving connection problems 106
About responding to emergencies 106
About monitoring protection features 108
About viewing details of system vulnerabilities 144

Chapter 4 Scanning your computer 149
About the Norton 360 scans 149
About Computer Scan 152

About Insight Network scan 168
About Reputation Scan 170
About Scan Facebook Wall 182
About SONAR Protection 185
About scanning Office documents 189
About Silent Mode 191
About boot time protection 204
Running a scan at the command prompt 205

Chapter 5 Responding to security issues 209
What to do if a security risk is found 209

Chapter 6 Understanding alerts and messages 219
About Norton 360 alerts and messages 219
About managing messages and alerts 219
Types of risks 221
Types of threats 222
Types of viruses 223

Chapter 7 Doing routine tasks 225
Turning on or turning off automatic tasks 225
About custom task 226
About scheduling automatic tasks 228
About scheduling backups 230
Specifying Idle Time Out duration 231

Chapter 8 Keeping secure on the Internet 233
About the Smart Firewall 233
About Intrusion Prevention 260
About Download Insight 269
About Norton AntiSpam 279
About configuring POP3 and SMTP ports 294
About Metered Broadband Mode 296

Chapter 9 Securing your sensitive data 301
About securing your sensitive data 301

Chapter 10 Protecting your home network 375
About the Network Security Map 375

Chapter 11 Keeping your PC tuned up 401
About PC Tuneup 401
About disk and file fragmentation 402
Optimizing your permanent disks manually 402
About using optimization efficiently 403
About cleaning up disk clutter 404
Running a scan to clean up disk clutter 405
Running Registry Cleanup 406
Running Diagnostic Report 406
About Startup Manager 407

Chapter 12 Protecting your media and data 411
About Norton Backup and Restore 411
About backups 412
About backup preparation 413
About backup set 417
Backing up your files 446
Restoring files 447
About Norton Backup Drive 456
About solutions to the backup problems 460
About online backup considerations 464
Turning off or turning on backup 469
Turning off or turning on backup setting options 471

Chapter 13 Customizing settings 475
About Norton 360 Settings 475
Customizing Norton 360 Settings 480
Turning on or turning off Quick Controls services 481

About Antivirus settings 482
About Firewall settings 506
About Norton AntiSpam settings 515
About My Network settings 519
About backup settings 521
About Identity Protection settings 524
About Task Scheduling settings 528
About Administrative Settings 532

Chapter 14 Finding additional solutions 553
Finding the version number of your product 553
Finding the End-User License Agreement 554
About upgrading your product 554
About Norton Autofix 557
Staying informed about protection issues 559
About Support 560
Uninstalling Norton 360 566

Index 569

Getting Started

1

This chapter includes the following topics:

- About Norton 360
- Activation protects you
- About your Norton Account
- About Norton Community Watch
- About Norton Bootable Recovery Tool
- About updating Norton 360
- About Network Proxy Settings
- About Norton 360 status

About Norton 360

Norton 360 offers proven performance and delivers today's fast and light all-in-one solution to protect your PC and all your online activities. It protects against viruses, worms, hackers, and botnet. With a single subscription, you can protect up to three PCs. It safeguards against online identity theft, protects important files, and keeps your PC tuned and running at peak performance.

Norton 360 is completely automated and easy to use. It works quietly in the background to maintain your overall system integrity with minimal effect on PC

performance. By offering an unmatched combination of performance and protection, Norton 360 helps you get the most out of your PC and your online experience.

About Norton 360 main window

The Norton 360 main window acts as a security management interface. You can access the main features and monitor the performance of your computer from the main window.

As you use your computer, Norton 360 monitors how well your computer and activities are protected from threats, risks, and damage. Norton 360 displays the protection status of your computer in the main window.

Depending on the security status of your computer, at the top left of the Norton 360 main window, Norton 360 shows your **System Status** as **Secure**, **Attention**, or **At Risk**. If your system status is marked as **Attention** or **At Risk**, at the bottom of the main window, click **Fix Now** to resolve all the security threats on your computer.

The options that are available in the main window summarize the most essential security and the productivity issues that challenge users. They are:

PC Security	Includes all virus, spyware, firewall, and other security features.
Identity	Includes the protection against phishing and fraudulent Web sites.
Backup	Includes the automatic and the customizable backups and restore capability.

PC Tuneup	Includes the performance tuning features, such as cleaning up unwanted files and performing Registry Cleanup .

Depending on the security status of the different components of your computer, the status areas of the four protection categories are marked as **Protected**, **Attention**, or **At Risk**.

When the **System Status** or protection categories statuses are marked as **At Risk** or **Attention**, at the bottom of the main window, click **Fix Now** to resolve all the security threats on your computer.

Norton 360 also provides you easy links at the top of the main window to the most frequent tasks. They are:

Tasks	Lets you access the **Tasks** window to run general tasks, backup tasks, and PC Tuneup tasks.
Settings	Lets you access the **Settings** window to configure settings such as Firewall, Antispam, and Backup.

Performance	Lets you open the **Performance** window in Norton 360. The **Performance** window chronicles all installs, downloads, optimizations, detections, alerts, and instances of Quick Scan that occurred on your computer since installing Norton 360. The window also displays a detailed graphical representation of the CPU and memory usage by your Norton product.
Feedback	Lets you give feedback about the Norton product that you use.
Account	Lets you access the **My Account** window to manage your Norton Account.
Support	Lets you access support options, product upgrade options, subscription status, and product version number. You can also access the online Help from the **Support** drop-down menu. Help provides links to information that assists you with the specific tasks that you want to complete. The online Help guides you to configure all of the product features.

The bottom section of the Norton 360 main window provides you up-to-date virus and threat information.

When your system status is **At Risk** or **Attention**, this section automatically provides you the **Fix Now** option to fix all the issues at once.

The bottom section of the Norton 360 main window helps you do the following:

Activity Map

Lets you access the world map with hotspots of cybercrimes and the latest threats.

The Activity Map shows the top cities in the world where most of the cybercrime activities occur. These cities are represented as yellow dots on the map. You can click a continent in the world map to view its cities with the highest number of threats. The details on the Activity Map are updated from a Symantec server on a regular basis. Your computer must be connected to the Internet to receive the activity map updates.

You can view the date and time that the Activity Map was last updated. You can also use the **Map Details** link to get a brief idea of the Activity Map.

When you click **Map Details**, the Activity Map shows a series of latest viruses and threats that your product protects your computer from. You can use the **info** link next to each item to view its details in an overlay window. You can also use the **View Details** link in the overlay window to know more about the threat in a Symantec Web page.

Manage	Lets you access Norton Management. Norton Management lets you manage your Norton products installed on all of your devices from one location. To sign up or to log into Norton Management, click the **Manage** icon at the bottom of the main window. You can use your existing Norton Account login information to access Norton Management. The Norton Management agent should be installed on each device that you want to add to Norton Management. Norton Management may not be available in some versions of Norton 360.
Mobile	Lets you download the Norton Mobile Security for Android. Norton Mobile Security helps protect your mobile devices against loss, theft, viruses, and other mobile threats. You can use Norton Mobile Security on all your devices that use the Android operating system. Norton Mobile Security may not be available in some versions of Norton 360.

Online Family

Lets you monitor your child's activities on the Internet.

Norton Online Family may not be available with some versions of Norton 360. In such case, you may not be able to access Norton Online Family options.

When you click **Online Family** icon on the main window, the bottom section of the Norton 360 main window displays Norton Online Family sign in options. Norton Online Family provides you advanced controls to monitor your child's online activities.

You can use the link on the bottom section of the Norton 360 main window to set up your account with Norton Online Family.

Symantec recommends that you use your Norton Account login credentials to sign in to Norton Online Family. If you register your product with your Norton Account, your Norton Account email address is auto-filled in the email address text box.

After you set up your account, you can sign in to your account on the bottom section of the Norton 360 main window and view your child's Internet activities. The bottom section of the Norton 360 main window shows details such as your child's

latest search terms, and the latest alerts. After you sign in, you can use the **Get Details** option in the bottom section of the Norton 360 main window to view more details on the Norton Online Family Web site.

Safe Web

Lets you check the safety of a Web site.

You can also perform a safe search.

This option may not be available with some versions of Norton 360. In such case, you may not be able to access this option.

When you click **Safe Web** icon on the main window, the bottom section of the Norton 360 main window displays Norton Safe Web options.

You can use the **Check Site** option in the bottom section of the Norton 360 main window to analyze the security levels of any Web site that you want to visit. When you type a Web site address in the text box and click **Check Site**, it shows the Symantec's ratings for the Web site.

You can use the **Safe Search** option in the bottom section of the Norton 360 main window to search for information on the Internet. The Norton Safe Search uses Ask.com to generate the search results. Norton Safe Search provides a site safety status and a Norton rating for each of the search results generated.

You can also use the **View recent Norton Safe Web**

activity option in the bottom section of the Norton 360 main window to view the recent Norton Safe Web statistics on malicious sites and URLs. You can also view the list of new malicious URLs.

Your activation status or subscription status appears at the bottom of the main window. You can use the **Activate Now** option to activate or subscribe your Norton product.

Activation protects you

Product activation protects users from pirated or counterfeit software. It protects you by limiting the use of a product to those users who have acquired the product legitimately. Product activation requires a product key for each installation of a product. You must activate the product within a limited time period after you install it.

If you are connected to the Internet, product activation takes place automatically when you start the product for the first time after installation. After activation, the **Norton Account** window appears. You can create your Norton Account and register your product.

If you are not connected to the Internet, you can click **Try Later** in the **Activation not complete** window to start your product. The **Activation** window reappears every time you start your product until you activate your product. If you choose not to activate at that time, you receive an alert that reminds you to activate the product. You can also activate your product by clicking the **Trial Period Status** link in the Norton 360 main window.

If you do not activate the product within the time period that the alert specifies, the product stops working. You can activate it after the time period has elapsed, but you are not protected until you activate the product.

Activating Norton 360

To use all of the features in Norton 360, you must first activate your product. Product activation reduces software piracy and ensures that you have authentic Symantec software. You can renew your subscription after the end of your subscription period.

If you are connected to the Internet, product activation takes place automatically when you start the product for the first time after installation. During activation, the **Norton Account** window appears. You can create your Norton Account and register your product. You can also view details, such as your Product Key and recent updates to the product. If you skip the **Norton Account** window, the product is activated, but the Product Key is not saved in the Norton Account. You can print the Product Key for the future, if you need to reinstall your product.

If you did not activate your product during installation, Norton 360 prompts for activation each time you start the product. Also, you receive an activation alert regularly until you activate the product.

You must activate your product within the time period that the alert specifies, or your product stops working.

You can activate your product directly from the activation alert. You can also activate your product from the **Trial Period Status** link in the main window or from the **My Account** window. In some cases, you might need to enter your Product Key to activate your product. You can activate or renew the subscription of your product from any non-admin user account as well. Activation should take only a few minutes.

To activate Norton 360, your computer must be connected to the Internet. If you use a proxy server to connect to the Internet, you must configure the proxy settings. To configure proxy settings, go to the Norton 360 main window, and then click **Settings > Administrative Settings > Network Proxy Settings > Configure**.

To activate Norton 360 from the alert

1. In the alert, click **Activate Now** or **Renew Now**.
2. Click **OK**.
3. Follow the on-screen instructions.
4. In the window that appears, click **Done**.

To activate your Norton 360 from the My Account window

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Activate Norton 360** or **Renew Subscription**.
   The **Renew Subscription** option is available if you have already activated your product.
3. Follow the on-screen instructions.
4. In the window that appears, click **Done**.

To activate your product from the main window

1. In the Norton 360 main window, do one of the following:
   - If you purchased a subscription version of a retail product, click **Activate Now**.
   - If the product came installed on your computer, click **Activate Online Now**.
   - If you want to renew the subscription of your product, click **Renew**.
2. Follow the on-screen instructions to activate or subscribe your product.

Where to find your product key

The product key is a unique key that helps you to install and activate the Symantec product on your computer.

The product key is a 25-character alphanumeric string that is shown in five groups of five characters each, separated by hyphens. The location of the product key varies depending on how you acquired the product.

The locations of the product key are as follows:

If you purchased a retail copy of the product on CD	The product key is either on a sticker on the CD sleeve or on an insert in the product package.
If you purchased the product on DVD	The product key is on the DVD package.
If you downloaded the product from the Symantec Store	The product key is stored on your computer as part of the download process and is included in the confirmation email from the Symantec Store.
If your computer came with the product already installed	The product key is provided as part of the activation process. Be sure to save your product key by creating or signing in to your Norton Account, or by printing the key. You may need the product key if you ever want to reinstall your product.
If you received a product key card	The product key is printed on the card along with instructions on how to use it. Be sure to save your product key by creating or signing in to your Norton Account. You need the product key if you ever want to reinstall the product.

If you are still unable to locate your product key, you can recover it using Norton Account	To recover or access your product key log on to https://account.norton.com. If you are not registered, register for Norton Account. You can find the product key on the **Products** tab in the **Norton Account** page.

About problems during activation

If you cannot connect to the Symantec servers to activate your product, first check your Internet connection. You then need to see if you have parental control software, either installed or through your ISP, that might block the connection.

A connectivity problem can occur if you use parental control software. If you suspect that parental controls might block the connection, you can configure the parental controls so that they do not block the activation procedure. You need to log in to your parental control software or to the Internet through your ISP as an administrator to change your configuration.

If you use a proxy server to connect to the Internet, you must configure the proxy settings. To configure the proxy settings, go to the Norton 360 main window, and then click **Settings > Administrative Settings > Network Proxy Settings > Configure**.

About your Norton Account

When you create a Norton Account, you can manage all of your Norton products in one place. You can store your product keys in your Norton Account and also buy additional product keys. You can also register your product with the Norton Account. It takes only a few

moments to create your Norton Account. You must be connected to the Internet to create a Norton Account.

After you create a Norton Account, you can access and manage your account information and product information from anywhere. It helps to reinstall your products and download the latest version of the products. If you install your product on more than one PC, you can use the same Norton Account. To access your Norton Account, go to the following URL:

https://account.norton.com

You can create a Norton Account in the following ways:

- During activation

  You can create your Norton Account and register your product from the **Norton Account** window that appears when you activate the product. You must provide your account information in the **Norton Account** window that appears.
- Any time after activation

  You can create a Norton Account from the **Access Norton Account** link available in the **My Account** window.

After you log in to your Norton Account, you can manage your product information with the following options:

Products	Saves the information for all of the Norton products that you own. The **Products** tab provides you the information about the Norton products that you own and the expiration date. You can click the arrow icon against a product for more information such as product key and the registration date. You can also buy a new product key to protect additional computers. You can use the **Update** option to check and download the latest product version using Norton Update Center.
Order History	Contains order information of the Norton products you bought from Norton online store.

Profile	Saves your account information and your billing details. The **Profile** options are: ▪ **Account Information** You can update your Norton Account information and your shipping address on the **Account Information** tab. After you update, click **Update** to save the changes. ▪ **Billing Information** You can save your credit card information and your billing address on the **Billing Information** tab. It makes it easier for saving online orders. After you update, click **Update** to save the changes. ▪ **Change Password** You can change your current Norton Account password on the **Change Password** tab.

You can use the icons at the bottom of your Norton Account Web page to access and use the following:

Norton Online Family	Norton Online Family monitors and manages your child's Internet activities and computer usage.

Norton Online Backup	Norton Online Backup provides a secure and easy-to-use online backup solution that safeguards your important data against system crash, accidental deleting, virus infection, and other disasters.
Norton Safe Web	Norton Safe Web checks the safety of a Web site and lets you perform a safe Web search.
Norton.com	The Symantec Web site provides more information about the various products of Symantec, the latest updates on Internet security, and various support options.
Norton Update Center	Norton Update Center checks and lets you download the latest version of your Norton product.

If you forget your Norton Account password, you can get a temporary password by clicking the **Forgot your password** link in the **Norton Account** sign-in Web page. You need to provide your email address. You need to use the same email address that you provided when you created your Norton Account. Symantec sends a temporary password to your email address. You can use the temporary password for a limited time period. You must reset your password after you log in to your Norton Account.

Creating a Norton Account

Your Norton Account stores the product key and the billing information of your product. You can also register your product with the Norton Account.

In addition, Norton Account helps you to do the following:

- Access the product key and other product information when you need it.
- Reinstall your Norton product.
- Buy additional product keys for your home or office.
- Check and download the latest version of the product by using Norton Update Center.
- Save online orders and update billing information.
- Manage your online backup.

Your computer must be connected to the Internet to create a Norton Account. If you use a proxy server to connect to the Internet, you must configure the proxy settings. To configure the proxy settings, go to the Norton 360 main window, and then click **Settings > Administrative Settings > Network Proxy Settings > Configure**.

You can also create a Norton Account when you activate your product. When you create your Norton Account from the product, your product gets registered in your account. If you have an existing Norton Account, you can provide the same email address in the **Norton Account** window in your product. This way, you can register your current product and add it to the list of Norton products in your existing Norton Account. If you upgrade your registered product to the latest available version, your product remains registered to the same Norton Account. In this case, you can continue using the same Norton Account login credentials.

Symantec products that are older than the 2006 product year do not appear in your Norton Account.

To create a Norton Account from the Norton Account Web page

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Access Norton Account**.
3. In the Norton Account Web page that appears, click **Sign up now**.
4. In the **Norton Account Sign Up** Web page, provide the details about your account information, and then click **Sign Up**.

To create a Norton Account and register your product after activation

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Access Norton Account**.
3. In the **Complete Your Activation** window, type your email address, and then click **Next**.
4. In the **Create your Norton Account** window, provide your account details, and then click **Next**.
   Your product information gets saved in your Norton Account only after you log in to your Norton Account.
5. In the window that appears, click **Done**.

To log in to your Norton Account and access your product information, visit https://account.norton.com.

Accessing your Norton Account

The product key for each Norton product is conveniently stored in your Norton Account. After you have created your Norton Account successfully, you can access your account from anywhere in the world. You can log in to your Norton Account any time by visiting the following URL:

https://account.norton.com

You can easily find and update your account, product, and billing information from your Norton Account.

You can also change your Norton Account password, if required. Your computer must be connected to the Internet to access your Norton Account.

Symantec products that are older than the 2006 product year do not appear in your Norton Account.

To access Norton Account

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Access Norton Account**.
3. In the Norton Account Web page that appears, type your email address and password, and click **Sign In**.

Creating a temporary password for Norton Account

If you forget the password of your Norton Account, you can create a temporary password to sign in to your Norton Account. The temporary password is sent to the email address that you provided when you created your Norton Account.

After you sign in to your Norton Account by using the temporary password, you are prompted to change your password.

To create a temporary password for Norton Account

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Access Norton Account**.
3. In the Norton Account Web page that appears, under **Forgot your password?**, click **Recover it here**.
4. In the **Forgot your Password** Web page, verify the email address that is provided in the **Email Address** text box, and then click **Continue**.
   A temporary password is sent to your email address. You can use this temporary password to sign in to your Norton Account.

About Norton Community Watch

Norton Community Watch helps in identifying new security risks by submitting selected security and application data to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. The collective efforts from Norton security product users help in quick identification of solutions for these threats and risks. Norton Community Watch improves user security and product functionality. In addition, it helps Symantec to analyze the execution, schedule, and efficiency of Norton-specific tasks and settings on your computer.

Norton Community Watch collects and submits the following types of data:

- Identified malicious software such as portable executable files and running processes
- Any Web site URL that your product identifies as fraudulent
- All the Web site URLs that you visited before the detection of a risk
- The applications and processes that run on your computer regularly and during any security risk detection
- Response instances that your computer sends to any potential security risk
- General system information and performance attributes from the computer
- General information about your computer such as idle time, standby, and screensaver settings

After the potential security risks are assessed from the submitted data, Symantec sends the information back to Norton 360. The Norton features such as Norton Insight and Insight Network use this information to identify files and processes at risk.

You should participate in Norton Community Watch submissions to provide valuable contribution to the entire community that uses Norton security products.

No personally identifiable information is exposed during data collection and submission. Symantec maintains an adequate level of protection for the collected information. The **Detailed Error Data Collection** option under **Norton Community Watch** in the **Administrative Settings** window lets you allow or deny the detailed data submissions. The detailed data may vary depending on the Norton-specific errors and components. You can configure the option to manage the data submissions.

Norton Community Watch collects and submits detailed data about the Norton-specific errors and components only. It does not collect or store any personal information of any user.

If you chose not to join Norton Community Watch when you installed your Norton product, you can turn it on later. You can use the **Norton Community Watch** option in the **Administrative Settings** window. You can also review the data, which Norton Community Watch collects and submits to Symantec, in the **Security History** window.

Turning off or turning on Norton Community Watch

You can use the **Norton Community Watch** option to send information about a suspicious file to Symantec for analysis. Symantec assesses the data to determine the new threats and their sources. The Norton features such as Norton Insight and Insight Network use the Symantec assessed information to detect the security threats.

Norton Community Watch collects and submits detailed data about the Norton-specific errors and components only. It does not collect or store any personal information of any user.

You can use Security History to review the information that has been sent to Symantec.

To turn off or turn on Norton Community Watch

1 In the Norton 360 main window, click **Settings**.

2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Administrative Settings** window, in the **Norton Community Watch** row, do one of the following:
   - To turn off Norton Community Watch, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Norton Community Watch, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**.

About Norton Bootable Recovery Tool

Norton Bootable Recovery Tool scans and removes viruses, spyware, and other security risks from your computer. Your computer might be infected with a virus if you experience any of the following symptoms:

- You cannot install Norton 360.
- You cannot start your computer.
- Your computer is extremely slow.

Norton Bootable Recovery Tool is integrated with Windows Preinstallation Environment (WinPE). Therefore, you can run Norton Bootable Recovery Tool only from a CD, DVD, or USB key. You must use Norton Bootable Recovery Tool Wizard to create the Norton Bootable Recovery Tool CD, DVD, or USB key.

You cannot run Norton Bootable Recovery Tool in WinPE for more than 72 hours. If you run Norton Bootable Recovery Tool for more than 72 hours, your computer restarts without any notification.

You can use the Norton Bootable Recovery Tool CD, DVD, or USB key to recover a computer that is infected with viruses and other security threats. This security program is not a replacement for continuous, real-time protection from viruses and latest security risks. To protect your computer from future infections, be sure

to install or continue using Norton 360 that you already purchased.

Norton Bootable Recovery Tool detects and resolves the following security threats:

Viruses	Programs that infect another program, boot sector, partition sector, or document by inserting themselves or attaching themselves to that medium. Most viruses just replicate; many also do damage.
Trojan horses	Programs containing malicious codes that are disguised as or hiding in something benign, such as a game or utility.
Hacking tools	Tools that are used by a hacker to gain unauthorized access to your computer. One type of hacking tool, a keystroke logger, tracks and records your individual keystrokes and can send this information back to the hacker.
Spyware	Programs that can scan systems or monitor activity and relay the information to other computers or locations in cyberspace.

Adware	Programs that facilitate the delivery of advertising content through their own window, or by using another program's interface.
Trackware	Programs that track system activity, gather system information, or track user habits, and relay this information to third-party organizations. The information that is gathered by such programs is neither personally identifiable nor confidential. Trackware programs are installed with the user's consent, and may also be packaged as part of other software that is installed by the user.

Downloading the Norton Bootable Recovery Tool Wizard

If your attempt to install a Norton product fails, you can download the Norton Bootable Recovery Tool Wizard. This easy-to-use wizard helps you create Norton Bootable Recovery Tool on a CD, DVD, or USB key. You can use Norton Bootable Recovery Tool to scan your computer and remove any security threats that prevent successful installation.

It is recommended that you download and install Norton Bootable Recovery Tool Wizard on a computer that does not have any security threats and create Norton Bootable Recovery Tool. If you create Norton Bootable Recovery Tool on an infected computer, there is a chance that the recovery CD, DVD, or USB key might get infected.

To use Norton Bootable Recovery Tool, you must use the product key of the Norton product that you purchased. If you use a trial version of Norton 360, you need to create a Norton Account to receive a product key to use Norton Bootable Recovery Tool.

You can download Norton Bootable Recovery Tool Wizard in one of the following ways:

- From the **Start** menu.
- From the Norton Support Web site.

To download the Norton Bootable Recovery Tool Wizard from the Start menu

1. On the Windows taskbar, do one of the following:
   - In Windows XP, click **Start > Programs > Norton 360 > Norton Recovery Tools**.
   - In Windows Vista or Windows 7, click **Start > All Programs > Norton 360 > Norton Recovery Tools**.
2. Follow the on-screen instructions.

To download the Norton Bootable Recovery Tool Wizard from the Internet

1. Open your Web browser, and go to the following URL:
   http://www.norton.com/recoverytool_n360
2. Follow the on-screen instructions.

To download the Norton Bootable Recovery Tool Wizard from Norton 360

1. In the Norton 360 main window, click **Scan Now**.
2. In the **Computer Scan** pane, do one of the following:
   - Click **Quick Scan**.
   - Click **Full System Scan**.
3. At the bottom of the scan window, next to **If you think there are still risks**, click **click here**.
4. In the **Norton Rescue Tools** Web page, click **Download Norton Bootable Recovery Tool**.
5. Follow the on-screen instructions.

Using the Norton Bootable Recovery Tool

If the installation of your Norton product fails, you can use the Norton Bootable Recovery Tool to scan and remove any security threats that prevent successful installation. If your computer is infected and you are not able to start your Windows operating system, you can use Norton Bootable Recovery Tool to remove threats and recover your computer.

Norton Bootable Recovery Tool is available on the product CD that you purchased. You can use the product CD as a recovery media.

To use Norton Bootable Recovery Tool, you must use the product key of the Norton product that you purchased. If you use a trial version of Norton 360, you need to create a Norton Account to receive a product key to use Norton Bootable Recovery Tool.

To use the Norton Bootable Recovery Tool

1. Insert the recovery media and start your computer from the recovery media.
   The recovery media can be a Norton Bootable Recovery Tool CD, DVD, USB key, or the product CD.
2. Read the **Norton License Agreement**, type your product key, and then click **I Agree**.
   If you use a non-QWERTY keyboard, use the **Virtual Keyboard** option to enter your product key.
3. In the **Norton Bootable Recovery Tool** window, click **Norton Advanced Recovery Scan**.
4. Click **Start Scan**.
5. After the scan is complete, remove the recovery media from the drive or USB port, and restart your computer.

About updating Norton 360

Norton 360 uses the Internet to automatically obtain updates to its virus definition files and its program

files. These updates continually enhance the technology that Norton 360 uses to keep your PC protected.

Automatic updates require an Internet connection. If you use a proxy server to connect to the Internet, you must configure the proxy settings in your product. If you do not normally keep your PC connected to the Internet, you can manually update Norton 360 after you connect to the Internet. Updating Norton 360 on a regular basis ensures that you have the latest definition updates and program updates.

About LiveUpdate

Symantec products download the latest definition updates and program updates regularly from Symantec servers. The definition updates protect your computer from the latest viruses and unknown security threats. Using the LiveUpdate technology, Symantec products help you to obtain and install these updates.

LiveUpdate takes little time to download and process the definition updates and program updates. You can choose Smart Definitions to minimize download time, installation time, and memory consumption as Smart Definitions are a subset of virus definitions. The **Smart Definitions** option is available on the **Scans and Risks** tab in the **Antivirus** settings window. You can cancel the LiveUpdate session at any time.

LiveUpdate obtains these updates for your computer by using your Internet connection. If your network uses proxy servers to connect to Internet, LiveUpdate uses the proxy settings in your product to download the latest updates. You can use the **Network Proxy Settings** option in the **Administrative Settings** window to configure the proxy settings of your network.

About Program and Definition Updates

LiveUpdate obtains program updates and definition updates for your computer by using your Internet connection.

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of the entire product. Program updates are usually created to extend the operating system or hardware compatibility, adjust a performance issue, or fix program errors. Program updates are released on an as-needed basis.

Some program updates may require that you restart your computer after you install them.

LiveUpdate automates the process of downloading and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the older files and downloaded definitions from the temporary folder after processing the updates.

Definition updates are the files that keep your Symantec products up to date with the latest antithreat technology. The definition updates that you receive depend on which product you use.

The type of definition updates that each of the Symantec products receive are as follows:

Norton AntiVirus, Norton AntiVirus Online	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats.

Norton Internet Security, Norton Internet Security Online	In addition to the virus and security risk updates, users of these products receive definition updates for security protection. For the products that contain protection against phishing, users receive definition updates against phishing. The security definition updates provide the latest predefined firewall rules, the updated lists of applications that access the Internet, Intrusion Prevention signatures, and Symantec spam definition files. These lists are used to identify unauthorized access attempts to your computer.
Norton 360, Norton 360 Online	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats. In addition, users of these products receive Symantec spam definition files and definition updates against phishing.

Norton Security Suite, Norton Business Suite	Users of these products receive the latest virus definitions from Symantec that protects your computer from all types of security threats. In addition, users of these products receive Symantec spam definition files and definition updates against phishing.

About Smart Definitions

Norton 360 downloads and installs virus definitions regularly to protect your computer from the latest security threats. For faster downloads and installation purpose, Norton 360 classifies these virus definitions into two sets.

The virus definitions are classified into the following two sets:

Complete Set	Contains all the virus definitions for each threat that is known to Symantec.

Core Set	Contains the most important virus definitions that are required for latest security threats as viewed by Symantec. The Core Set is a subset of the Complete Set, and it is approximately 30 percent smaller than the Complete Set. The Core Set minimizes download time, installation time, and system start time. It also occupies lesser amount of disk space as compared to the Complete Set virus definitions. Therefore, the Core Set results in faster performance of your computer.

The Core Set virus definitions are called as Smart Definitions. Norton 360 provides the **Smart Definitions** option to choose between Core Set virus definitions and Complete Set virus definitions for LiveUpdate sessions. The option is available on the **Scans and Risks** tab in the **Antivirus** settings window.

During Automatic LiveUpdate or each time that you run LiveUpdate manually, Norton 360 checks if the **Smart Definitions** option is turned on or off. It then downloads and installs the desired set of virus definitions based on the option settings. By default, the **Smart Definitions** option is turned on, which means that the Core Set virus definitions are downloaded and installed.

Turning off or turning on Smart Definitions

Smart Definitions are a subset of virus definitions that contains most important definitions for the latest security threats.

As the Smart Definitions are of considerably smaller size, it results in lesser download time, lesser

installation time, lesser boot time, and lesser memory consumption. It also occupies lesser amount of disk space as compared to the full set of virus definitions. Therefore, Smart Definitions result in faster performance of your computer.

Norton 360 checks the **Smart Definitions** option settings during each LiveUpdate session. If the option is turned on, the Smart Definitions are downloaded and installed. If the option is turned off, all of the virus definitions are downloaded and installed.

To turn off or turn on Smart Definitions

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click the **Scans and Risks** tab.
4. In the **Smart Definitions** row, do one of the following:
   - To turn off Smart Definitions, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Smart Definitions, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **Close**.

Turning off or turning on Automatic LiveUpdate

You can have LiveUpdate check for definition updates and product updates automatically on a set schedule, by turning on the **Automatic LiveUpdate** option. You can also run LiveUpdate manually when the **Automatic LiveUpdate** option is turned on. However, you must run LiveUpdate manually to obtain updates if you have turned off the **Automatic LiveUpdate** option.

To access the **Automatic LiveUpdate** option, go the Norton 360 main window and then click **Settings > Antivirus > Antispyware and Updates**. You can also

turn off or turn on the **Automatic LiveUpdate** option from **Quick Controls** in the **Settings** window.

If you are connected to the Internet, Automatic LiveUpdate downloads product updates and definition updates every hour. If you have an Integrated Services Digital Network (ISDN) router that is set to automatically connect to your Internet service provider (ISP), it may incur charges each time. If you do not want this setup, you can turn off the automatic connection on your ISDN router, or turn off the **Automatic LiveUpdate** option.

To turn on Automatic LiveUpdate from Quick Controls

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, check **Automatic LiveUpdate**.

To turn off Automatic LiveUpdate from Quick Controls

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, uncheck **Automatic LiveUpdate**.
3. In the **Select the duration** drop-down list, select how long you want to turn off Automatic LiveUpdate, and then click **OK**.

Checking for updates manually

If you disconnect your PC from the Internet, Symantec recommends that you check for Norton 360 updates after you reconnect.

To check for updates manually

1. In the Norton 360 main window, click **PC Security**, and then click **Run LiveUpdate**.
2. In the **Norton LiveUpdate** window, when the LiveUpdate is completed successfully, click **Close**.

Checking for the latest virus and spyware definitions date

Virus definition files contain the information that allows Norton 360 to recognize and alert you to the

presence of a specific virus or security threat. Norton 360 shows the date on which you last updated the virus and spyware definitions.

You can also check the latest virus definition date. The **Definitions Update** section in the **PC Security Details** window displays the status and date of the last virus definition updates.

To check for the latest virus and spyware definition date

1. In the Norton 360 main window, click **PC Security**, and then click **View Details**.
2. In the **PC Security Details** window, under **Definitions Update**, view the latest virus definitions details.
   The **Status** column shows the date on which you last downloaded and installed the latest definition updates.

About keeping your protection up to date

Definition updates are available to you as long as you maintain an active product status. The ways in which you can acquire the product and maintain your status are as follows:

If you purchased a subscription version of a retail product	The product includes a limited-time subscription to definition updates. When the subscription is due to expire, you are prompted to renew. Follow the on-screen instructions to complete your subscription renewal. After your product expires, you cannot obtain updates of any kind and all the security features are turned off. If you do not renew your product, you are no longer protected against security threats. Though LiveUpdate continues to check for updates after expiration, you must renew your product to enable all the security features.

If you purchased a product as a service, or it came installed on your computer	If you do not activate your service or renew your subscription, you cannot obtain updates of any kind and the software no longer functions.
If you receive this service through your service provider	Your product status is always active as long as your security service is active with your service provider. If your security service is not active, you cannot obtain updates of any kind and the software no longer functions.

About Pulse Updates

In addition to the definition updates that Automatic LiveUpdate downloads, Norton 360 uses streaming technology to download the latest virus definitions. These downloads are called Pulse Updates. The Pulse Updates are lighter and faster than Automatic LiveUpdate. They keep your computer secure from the ongoing threats that exist on the Internet. Pulse Updates protect you against the rapidly-changing environment of security threats without compromising your computer's performance. Pulse Updates should always be turned on to get the latest updates.

Pulse Updates checks for definition updates every 5 minutes. If definition updates are available, LiveUpdate downloads the streamed virus definitions. Pulse Updates provide the updates in between the full updates, which Automatic LiveUpdate downloads automatically every hour. Norton 360 merges the new stream that is downloaded with the last updates that are installed. The Pulse Updates downloads provide additional and fast protection for the latest threats in between the full updates without disrupting your online experience.

Even if you do not turn on Pulse Updates, LiveUpdate collects all the missed streams and, it updates your computer during full definition updates.

Turning off or turning on Pulse Updates

Pulse Updates provide frequent, lightweight updates every 5 minutes in between the full updates. Always ensure that the **Pulse Updates** option is turned on. It protects you from the latest threats without compromising your system performance or disrupting your online experience.

You must be connected to the Internet to obtain latest definition updates by using Pulse Updates. You can turn on or turn off **Pulse Updates** only if **Automatic LiveUpdate** is turned on.

To turn off or turn on Pulse Updates

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click **Antispyware and Updates**.
4. Under **Automatic LiveUpdate**, in the **Pulse Updates** row, do one of the following:
   - To turn off Pulse Updates, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Pulse Updates, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.
6. Click **Close**.

About Network Proxy Settings

A proxy server regulates access to the Internet, and prevents external computers from accessing your network. If you are on a network that uses a proxy server to connect to the Internet, you can provide proxy server details to Norton 360. You can use the **Network**

Proxy Settings window to specify the automatic configuration URL, the proxy settings, and the authentication details. Norton 360 uses the proxy settings and authentication details to connect to the Internet automatically, whenever required. For example, LiveUpdate uses the specified proxy server settings to retrieve updates. You must ensure that you specify the proxy server details for LiveUpdate to run successfully.

In some cases, your network uses an automatic configuration URL or script for managing Internet access. In this case, you must provide the URL of the required Proxy Automatic Configuration (PAC) file. A PAC file contains the code that lets your browser know about the proxy settings for different Web sites over the Internet. It also contains the words which you want to filter and block while you access the Internet. You can also choose the option that lets your browser to automatically detect the proxy settings. If you want your manual settings in the network, ensure that you disable the **Automatic Configuration** options.

Network Proxy Settings window lets you specify the following settings:

Automatic Configuration	Lets you specify the automatic configuration URL or script to manage Internet access. You have the following options: ▪ **Automatically detect settings** Lets your browser detect the network settings automatically. If you do not want to override your manual settings for network connections, you must disable this option. ▪ **Use automatic configuration script** Lets your browser use the automatic configuration URL or script to manage Internet access. Use the **URL** box to provide the HTTP URL or the script to the required PAC file (such as file://C:/Proxy.pac).

Proxy Settings	Lets you provide the details of your Proxy Settings. Under **Proxy Settings**, check **Use a proxy server for your HTTP connections**, and do the following: ▪ In the **Address** box, type the URL or IP address of your proxy server. ▪ In the **Port** box, type the port number of your proxy server. You can specify a value from 1 to 65535.
Authentication	Lets you connect to the Internet through a server that requires authentication. Use the **Username** box and **Password** box to type the authentication details.

Configuring Network Proxy Settings

When you use a proxy server to connect to the Internet, you must specify the proxy server details. The **Network Proxy Settings** window lets you enter automatic configuration settings, proxy settings, and proxy server authentication settings. The Network Proxy settings let you connect to the Internet while you perform tasks such as activating the product or accessing the support options.

To configure Network Proxy Settings

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Network Proxy Settings** row, click **Configure**.

4 In the **Network Proxy Settings** window, do the following:

- If you want your browser to automatically detect network connection settings, under **Automatic Configuration**, check **Automatically detect settings**.
- If the proxy server requires an automatic configuration URL, under **Automatic Configuration**, check **Use automatic configuration script**. Type the URL (such as file://C:/Proxy.pac) in the **URL** box.
- If your network uses a proxy server, under **Proxy Settings**, check **Use a proxy server for your HTTP connections**. In the **Address** box, type the URL or IP address of your proxy server, and in the **Port** box, type the port number of your proxy server. You can specify a value from 1 to 65535.
- If your proxy server requires a user name and password, under **Authentication**, check **I need authentication to connect through my firewall or proxy server**. Type the user name in the **Username** box and password in the **Password** box.

5 In the **Network Proxy Settings** window, click **Apply**.

About Norton 360 status

Norton 360 displays the security status of your computer at the top of the main window. Based on the security status of your computer, Norton 360 shows your system status as **Protected**, **Attention**, or **At Risk**.

The system status indicator displays one of the following statuses:

Protected	Indicates that your computer is protected from threats, risks, and damages.

Attention	Indicates that your computer requires attention. At the bottom section of the Norton 360 main window, click **Fix Now** to resolve the security threats on your computer.
At Risk	Indicates that your computer is at risk. At the bottom section of the Norton 360 main window, click **Fix Now** to resolve the security threats on your computer.

Norton 360 displays individual security status for each protection category, such as PC Security, Identity, Backup, and PC Tuneup. Based on the security status of the different components of your computer, the status areas of the four protection categories are marked as **Protected**, **Attention**, or **At Risk**.

See "Responding to security status indicators" on page 53.

When your system status or protection categories statuses are marked as **At Risk** or **Attention**, at the bottom section of the Norton 360 main window, click **Fix Now** to resolve all the security threats on your computer.

Responding to security status indicators

When your system encounters a threat or a risk, the product displays the security status at the top of the main window. When a status indicator displays a status, you can take appropriate action to improve your protection status. Your protection is based on the programs that are installed on your computer. To improve your protection status, ensure that your installed programs are up to date.

When your system status or protection categories statuses are marked as **At Risk** or **Attention**, you can resolve the security issues directly from the main window.

To respond to security status indicators

1. In the Norton 360 main window, click **Fix Now**.
2. Follow the on-screen instructions.

About the Norton 360 icon

When you install Norton 360, it places an icon in the notification area at the far right of the taskbar. This icon indicates the current security status of your computer. Norton 360 displays an animated icon when it actively fixes any issues or wants to inform you about any warning or urgent issues.

You can see the following representations of Norton 360 icon in the notification area:

Icon with a green check mark badge	Represents that your computer is fully protected
Icon with an orange exclamation mark badge	Represents that there are some issues against your computer protection that require your attention
Icon with a red cross mark badge	Represents that there are some urgent issues against your computer protection that require immediate resolution
Icon with a crescent-shaped edge	Represents that the Silent Mode feature is turned on This icon also displays the current protection status badge.

You can right-click the icon to see a shortcut menu for Norton 360. You can choose items on the shortcut menu to open the Norton 360 window, to fix any issues that Norton 360 detects, or to get additional help.

About Norton 360 shortcut menu

Norton 360 works in the background to keep your PC secure. The Norton 360 icon is available in the notification area at the far right of the taskbar. The icon reassures you that your protection is up to date. It changes its color if any change in status occurs.

The messages that appear in the notification area may require a response from you, such as opening a window. More often, messages inform you about current activities, and they disappear after a few seconds.

You can right-click the **Norton 360** icon to access specific Norton 360 activities. Depending on the current activities, your options include the following:

Open Norton 360	Use this option to launch the Norton 360 main window to complete tasks, view current status, or access other features.
Run QuickScan	Use this option to run a Quick Scan to protect possible virus-infected areas of your computer.
Run LiveUpdate	Use this option to run LiveUpdate to check for definition updates and program updates.

Run Backup Now	Use this option to create a backup of your files. You can specify when and how often Norton 360 backs up your files.
View Recent History	Use this option to review the information about the security events for all of the categories.
Get Support	Use this option to resolve your problem easily using Norton Autofix.
Turn on/Turn off Silent Mode	Use this option to turn on or turn off Silent Mode.
Enable/Disable Smart Firewall	Use this option to turn on or turn off the firewall.
Enable/Disable Antivirus Auto-Protect	Use this option to turn on or turn off Antivirus Auto-Protect.
Check for New Version	Use this option to check and download the latest version of the product.

Viewing details of protection features

In the Norton 360 main window, you can see a summary of each of the four protection features that Norton 360 provides. You can view additional details about each protection feature.

To view details of a protection feature

1. In the Norton 360 main window, click on a protection feature, and then click **View Details**. In the window that appears, you can view the following details:
   - The current status of the protection feature.
   - A list of the checks that the feature performs, and the results of each check. In some cases, the results of a check can include a link that provides additional information.
   - A list of actions that you can perform.
2. After you view details, click **Close**.

Monitoring your system's performance

2

This chapter includes the following topics:

- About System Insight

About System Insight

Norton 360 continuously monitors your computer to keep it free of any problems and run at peak efficiency. Norton 360 constantly scans the vital areas of your computer including memory, registry keys, and running processes. It monitors the important activities such as general file operation, network traffic, and Internet browsing. In addition, Norton 360 ensures that the activities that it performs on your computer do not degrade the overall performance of your computer.

System Insight provides you a centralized location where you can view and monitor the activities that you perform on your system. System Insight displays such information in the **Performance** window.

You can use the **Performance** window for the following:

- To view monthly history of the important system activities that you performed or that occurred over a period of the last three months.

  The Events graph that appears at the top of the window provides a pictorial representation of important system activities. The activities include application installations, application downloads, disk optimizations, threat detections, performance

alerts, or Quick Scans. The graph displays the activities as icon or stripe, and the description for each icon or stripe is provided at the bottom of the graph. The pop-up that appears when you move the mouse pointer over an icon provides you the details about the activity. The **View Details** link in the pop-up lets you view additional details about the activity in the **Security History** window. You can use the tabs at the top of the graph to obtain details for the current month and details for the last two months.

- To rearrange the organization of files on your computer.

  Optimizing your system helps you maximize the usable free space on a disk by grouping files based on how they are accessed. The **Optimize** option at the top of the Events graph lets you defragment your system.
- To view and analyze the effect of Norton 360 on the performance of your computer.

  The Performance graph that appears at the bottom of the window provides a graphical representation of your CPU usage and memory usage. The **CPU** tab displays a graph that represents the overall system CPU usage and Norton-specific CPU usage. When you click at any point on the CPU graph and memory graph, Norton 360 displays a list of the processes that consume maximum resources at that point. It also displays the percentage of usage for each process. You can click a process that is available in the list to get more information about the process in the **File Insight** window. The **Memory** tab displays a graph that represents overall memory usage and Norton-specific memory usage. You can select any of the **Zoom** options to obtain magnified view or historical data of the graphs.
- To view the details of Norton-specific jobs that are currently running in the background

The **Norton Tasks** window provides the details such as the timestamp, the duration, and the status of the background jobs. The details also include the type of power the job needs to run and if a job ran during idle time. You can select different power sources for the background jobs. You can also start or stop a background job at any time.

- To view details about the known good files and the known bad files

  The **Norton Insight Network** window lets you view the total number of files that Symantec analyzes within the Norton Community. You can also view the total number of computers that are available in the community to provide the data. You can view the number of trusted files that are available on your computer.

- To view the details of the Files of Interest

  The **Norton Insight - Application Ratings** window provides details on the trust level, prevalence, resource usage, and stability ratings for the Files of Interest.

You can use the **Performance Monitoring** option to monitor the performance of your computer. To access the **Performance Monitoring** option, go to the Norton 360 main window, click **Settings > Administrative Settings > Performance Monitoring**.

Accessing the Performance window

System Insight provides you a centralized location where you can view and monitor your system activities. System Insight displays such information in the **Performance** window. You can access the **Performance** window to view details about the important system activities, CPU usage and memory usage, and Norton-specific background jobs. You can also view Norton Insight details and defragment your boot volume.

To access the Performance window

- In the Norton 360 main window, click **Performance**.

About monitoring system activities

System Insight provides information about the important system activities that you performed or that occurred over a period of the last three months. System Insight displays the information in the **Performance** window. The Events graph at the top of the **Performance** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. You can use the tabs at the top of the graph to obtain details for the current month and for the last two months. The activities include:

Installs	Provides the details about the installation activities that you performed on your system over a period of the last three months The details include the application that you installed, the date on which you installed the application, and the total number of installations on that date.

Downloads	Provides the details about the application-download activities that you performed on your system over a period of the last three months The details include the date on which you downloaded a file and the total number of downloads on that date. You can click the file name link to view additional details about the downloaded file such as the Download Insight report, file name, reputation level, and recommended action.
Optimized	Indicates the optimization activities that you performed on your system over a period of the last three months
Detections	Provides the details about the threat detection activities that Norton 360 performed on your system over a period of the last three months The details include the date on which Norton 360 detected a threat and the total number of threats that Norton 360 detected on that date. The **View Details** link provides additional details about the risk such as the risk impact and the origin of the risk. The details also include the action that a threat has performed on your system and the action that Symantec recommends you to resolve the threat.

Alerts	Provides the details about the performance alerts that Norton 360 displayed over a period of the last three months The details include the monitored date and the number of performance alerts generated. The **View Details** link provides additional details about performance-related activities, program name, program location, and system resources utilization.
Quick Scans	Provides the details about Quick Scans that Norton 360 performed on your system over a period of the last three months The details include the date on which a Quick Scan was performed and the number of Quick Scans that were performed on that date. The **View Details** link provides additional details such as the scan time, total items scanned, total risk detected, total risks resolved, and recommended action.

Viewing details of your system activities

System Insight lets you view details of the system activities that you performed or that occurred over the last three months in the **Performance** window. The activities include application installations, application downloads, disk optimizations, threat detections, performance alerts, or Quick Scans. You can use the tabs at the top of the Events graph to obtain details for the current month and for the last two months. The

Events graph at the top of the **Performance** window displays each activity as icon or stripe. The description for each icon or stripe appears at the bottom of the graph. The pop-up that appears when you move the mouse pointer over an icon provides you the details about the activity. The details include the date on which an activity was performed and the number of such activities that you performed on that date. The **View Details** link provides additional details of the activity in the **Security History** window.

To view details of your system activities

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, at the top of the Events graph, click the tab for a month to view the details.
3. In the Events graph, move the mouse pointer over the icon or the stripe for an activity.
4. In the pop-up that appears, view the details of the activity.
5. If the **View Details** option appears in the pop-up, click **View Details** to view additional details in the **Security History** window.

About performance alerting

Norton 360 monitors your system performance. If it detects an increased usage of system resources by any program or process, it notifies you with performance alerts. Performance alerting works only when the **Performance Monitoring** option and **Performance Alerting** option are turned on.

Performance alerting notifies you with information about the program name and resources that the program uses excessively. The **Details & Settings** link in the performance notification alert lets you view additional details about the resource consumption by the program. The **File Insight** window opens and displays the details of the file, the origin of the file, the process ID, and the complete resource usage list of the program. From the **File Insight** window, you can choose

to exclude the program from being monitored. You can use the **Settings** option in the **File Insight** window to turn off the **Performance Alerting** option.

Performance alerts are not displayed when your computer is idle or in Silent Mode.

For each system resource, such as CPU, memory, and hard disk, there is a resource consumption threshold defined. When the resource consumption of a program exceeds the defined threshold limit, Norton 360 alerts you with a performance alert.

You can use the **Resource Threshold Profile for Alerting** option to configure the threshold limit. To access the **Resource Threshold Profile for Alerting** option, go to the Norton 360 main window, and then click **Settings > Administrative Settings > Performance Monitoring > Resource Threshold Profile for Alerting**.

You can use the **Use Low Resource Profile On Battery Power** option to let Norton 360 automatically change the resource threshold profile to low when your computer runs on battery power.

You can use **High-Usage Alert for** option to configure Norton 360 to alert for high usage of CPU, memory, disk, and handles.

In addition, you can add programs to the **Program Exclusions** list using the **Program Exclusions** option. When you add a program to the **Program Exclusions** list, Norton 360 does not alert you when the program exceeds the defined resource consumption threshold limit.

You can view all the performance-related logs under the **Performance Alert** category in the **Security History** window.

Configuring performance alerts

You can use the **Performance Alerting** option to receive performance alerts when there is an increased usage of system resources by any program or process.

You can use the following options to configure performance alerts:

Off	Turns off performance alerts. Select this option if you do not want Norton 360 to notify you with performance alerts.
On	Turns on performance alerts. Select this option if you want Norton 360 to notify you with performance alerts when a program or process exceeds the threshold limit of the system resource usage. By default, the **Performance Alerting** option is turned on.

Log Only	Monitors and records the system resource usage. Select this option if you want Norton 360 to only monitor the system resource usage of every program or process running on your computer. When a program or process exceeds the threshold limit of the system resource usage, Norton 360 records these details in the **Security History** window. You can view the details that are related to performance alerts under **Performance Alert** category in the **Security History** window.

To configure performance alerts

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Performance Alerting** row, do one of the following:
   - To turn off performance alerts, move the **Performance Alerting** switch to the **Off** position.
   - To turn on performance alerts, move the **Performance Alerting** switch to the **On** position.
   - To suppress the performance alerts, move the **Performance Alerting** switch to the **Log Only** position.

4 Under **High-Usage Alert for**, do one of the following:
   - If you want Norton 360 to monitor the CPU usage, move the **CPU** switch to the left to the **On** position.
   - If you want Norton 360 to monitor the memory usage, move the **Memory** switch to the left to the **On** position.
   - If you want Norton 360 to monitor the disk usage, move the **Disk** switch to the left to the **On** position.
   - If you want Norton 360 to monitor the handle count, move the **Handles** switch to the left to the **On** position. By default, this option is turned off.
5 Click **Apply**, and then click **Close**.

Configuring the resource threshold profile

The threshold limit for the system resources determines at which point Norton 360 should notify you with performance alerts. When a specific program exceeds the threshold limit of using your system resource, Norton 360 notifies you with a performance alert.

To configure the resource threshold profile

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.

3 Under **Performance Monitoring**, in the **Resource Threshold Profile for Alerting** row, select one of the following options:

Low	Configures a low threshold limit for alerting. Symantec recommends you to select this option when your computer runs on battery power.
Medium	Configures a medium threshold limit for alerting. By default, the threshold limit is set to medium.
High	Configures a high threshold limit for alerting. Symantec recommends you to select this option when your computer runs tasks that require high resource.

4 Click **Apply** and then click **Close**.

Turning off or turning on the Use Low Resource Profile On Battery Power option

When your computer runs on battery power, it is important that all active software programs consume minimum resource usage. By reducing resource usage, your computer gains longer battery life and becomes more energy efficient.

You can configure a low threshold profile and ensure that all programs consume minimum resource usage. When the resource usage of a program or a process exceeds the low threshold limit, Norton 360 notifies you with a performance alert. You can choose to close

the program or the process manually and free the resource.

If the **Use Low Resource Profile On Battery Power** option is turned on, Norton 360 automatically changes the threshold profile to low when your computer runs on battery power. By default, this option is turned on.

Symantec recommends that you keep the **Use Low Resource Profile On Battery Power** option turned on.

To turn off the Use Low Resource Profile On Battery Power option

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**, and then click **Close**.

To turn on the Use Low Resource Profile On Battery Power option

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Use Low Resource Profile On Battery Power** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

Excluding programs from performance alerts

Norton 360 lets you exclude programs from performance alerts. You can add the programs that consume high CPU, memory, or disk usage to the **Program Exclusions** list. When you add a program to the **Program Exclusions** list, Norton 360 does not alert you when the program exceeds the resource consumption threshold limit.

To exclude a program from performance alerts

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
4. In the **Program Exclusions** window, click **Add**.
5. In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
6. Click **Open**.
7. In the **Program Exclusions** window, click **Apply**.
8. Click **OK**.
9. In the **Settings** window, click **Apply**.
10. Click **Close**.

Removing programs from Program Exclusions

The **Program Exclusions** window lists all the programs that are excluded from performance alerts. If you want, you can remove any of the programs that you already added to the **Program Exclusions** window. When you remove a program, the program appears in the performance alert the next time it crosses the defined threshold limit for resource consumption.

To remove a program from Program Exclusions

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Performance Monitoring**, in the **Program Exclusions** row, click **Configure**.
4. In the **Program Exclusions** window, select the program that you want to delete, and then click **Remove**.
   To remove all the programs available in the **Program Exclusions** window, click **Remove All**.
5. In the **Program Exclusions** window, click **Apply**

6 Click **OK**.

7 In the **Settings** window, click **Close**.

About CPU graph and memory graph

Norton 360 monitors the overall system CPU usage and memory usage and the Norton-specific CPU usage and memory usage. Norton 360 displays the details in the CPU graph and the memory graph. The CPU graph and memory graph are real-time graphs of CPU utilization and memory utilization.

The graphs display a performance time for the last 90 minutes or for the duration since you started your computer. The graphs update the information at an interval of every 15 seconds. The graphs progress from right to left, and the most recent data appear on the far right of the graph. The blue pattern in the graphs depicts the overall system usage, and the yellow pattern depicts the Norton-specific usage. The gray blocks that are labeled as **Idle** indicate the idle period of your computer. The gray blocks include the period when your computer is in shutdown, sleep, or log out state.

The graphs show a default performance time of 90 minutes. However, you can use the **Zoom** options to define a region of the graph that you are interested to view. You can select a **Zoom** option to obtain magnified view or historical data of the graphs. For example, if you select the **10min** option, Norton 360 displays the magnified view of CPU graph or memory graph for the last 10 minutes. If you select the **1D** option, Norton 360 displays a historical data of the last one day.

When you click at any point on the CPU graph or memory graph, Norton 360 displays a list of the processes that consume maximum resources at that point. It also displays the percentage of usage for each process. You can click a process that is available in the list to get more information in the **File Insight** window.

The **File Insight** window provides information about the process such as:

- The file name, version number, digital signature, the date on which the process was installed.
- The date on which the process was last used and whether it is a startup file.
- The stability details.
- The confidence level.
- The resource usage details.
- The actions that the process performs on your system.

In addition, the **File Insight** window displays the CPU graph and the resource usage details for the running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage by the process.

Viewing the CPU graph and memory graph

Norton 360 monitors the overall system CPU usage and memory usage and the Norton-specific CPU usage and memory usage. The **CPU** tab and the **Memory** tab at the top of the Performance graph display the CPU graph and the memory graph respectively.

The **Zoom** options provide you the magnified view of the CPU graph and memory graph. For example, if you select the **10min** option, Norton 360 displays the magnified view of CPU graph or memory graph for the last 10 minutes. If you select the **1W** option, Norton 360 displays the CPU graph and memory graph for the last one week.

By default, the graphs display performance time for the last 90 minutes.

To view CPU graph and memory graph

1 In the Norton 360 main window, click **Performance**.

2 In the **Performance** window, do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
   - To magnify or shrink the graph, click **10min, 30min, 1D, 1W,** or **1M** next to the **Zoom** option.

Obtaining historical data of your CPU and memory usage

The **Zoom** options also provide you the historical data of the CPU graph and memory graph. For example, if you select the **1D** option, Norton 360 displays the data of CPU graph or memory graph for the last one day.

To view historical data of your CPU or memory usage

1 In the Norton 360 main window, click **Performance**.
2 In the **Performance** window, do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
3 Do one of the following:
   - To obtain historical data for the last one day, click **1D**.
   - To obtain historical data for the last one week, click **1W**.
   - To obtain historical data for the last one month, click **1M**.

Identifying resource-consuming processes

You can click at any point on the CPU graph or memory graph to obtain a list of top three processes that consume maximum resources of your computer at that point. You can click a process that is available in the list to get more information about the process in the **File Insight** window.

To identify resource-consuming processes

1 In the Norton 360 main window, click **Performance**.

2 In the **Performance** window, do one of the following:
   - To view the CPU graph, click the **CPU** tab.
   - To view the memory graph, click the **Memory** tab.
3 Click at any point on the graph to obtain a list of resource-consuming processes.
4 Click the name of a process to obtain additional information about the process in the **File Insight** window.

About optimization

The data storage space on a disk is divided into discrete units. These units are called clusters. When files are written to the disk, they are broken up into cluster-sized pieces. When all of the file pieces are located in adjacent or contiguous clusters, the file can be accessed quickly.

Your computer's hard disk stores all of your files, applications, and the Windows operating system. The bits of information that make up your files gradually spread over the disk. This process is known as fragmentation. The more that you use your computer, the more fragmented the hard disk gets.

When a fragmented file is accessed, the disk performance is slower. The performance is slower because the drive head locates, loads, saves, and keeps track of all of the fragments of the file. If free space is also fragmented, the drive head might have to track adequate free space to store temporary files or newly added files.

Optimization rearranges file fragments into adjacent or contiguous clusters. When the drive head accesses all of the file data in one location, the file is read into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. Optimization consolidates free space to avoid fragmenting newly added files. It adds extra space after major data

structures so that they can grow without immediately becoming fragmented again.

You can optimize your boot volume manually by using the **Optimize** option in the **Performance** window.

You can also configure Norton 360 to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Norton 360 automatically schedules the optimization when it detects the installation of an application on your computer. The optimization process starts next time when your computer is idle.

You can use the **Idle Time Optimizer** option in the **Administrative Settings** window to optimize the boot volume during idle time.

Optimizing your boot volume

The **Optimize** option lets you optimize your boot volume to improve the boot time of your computer. Optimization of your boot volume maximizes the usable free space by rearranging file fragments into adjacent and contiguous clusters. When the drive head of your hard disk accesses all of the file data in one location, the file is read into the memory faster.

When you use the **Optimize** option in Windows XP, Norton 360 optimizes only the boot volume (for example, C:\Windows). Therefore, it requires less time to complete optimization. However, when you use the **Optimize** option in Windows Vista or Windows 7, Norton 360 optimizes the drive that contains the boot volume. Therefore, it requires more time to complete optimization.

You can access the **Optimize** option at the top of the security status graph in the **Performance** window. You can also optimize your boot volume using the **Insight Optimizer** option in the **Norton Tasks** window. The **Insight Optimizer** row in the background jobs list that is available in the **Norton Tasks** window displays the details of the boot volume optimization process. You

can view details such as timestamp, duration, and status of the background job.

To optimize your boot volume from the Performance window

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, at the top of the security status graph, click **Optimize**.

To optimize your boot volume from the Norton Tasks window

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.
3. In the **Norton Tasks** window, under the **Norton Tasks** column, click the play icon that appears before **Insight Optimizer**.

About the Idle Time Optimizer

Idle Time Optimizer lets you configure Norton 360 to defragment your boot volume or the local disk that contains boot volume when your computer is idle. Norton 360 automatically schedules the optimization when it detects the installation of an application on your computer and your computer is idle. If you start using your computer again, Norton 360 stops the optimization task, and starts optimizing the next time that your computer is idle. This way, the background job of optimization does not affect the performance of your computer.

Optimization rearranges file fragments into adjacent or contiguous clusters in the hard disk. It improves the computer performance by reading the files into the memory faster. Optimization also maximizes the usable free space on a disk by grouping most frequently used files and infrequently used files. In addition, it consolidates free space to avoid fragmenting newly added files.

You must turn on the **Idle Time Optimizer** option under **Administrative Settings** in the **Settings** window

to optimize the boot volume during idle time. By default, this option is turned on.

Turning off or turning on Idle Time Optimizer

Norton 360 automatically schedules the optimization when it detects the installation of a new application on your computer. Norton 360 runs this optimization only when your computer is idle.

You can use the **Idle Time Optimizer** option to optimize the boot volume during idle time. By default, this option is turned on.

To turn off Idle Time Optimizer

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Optimizer** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**, and then click **Close**.

To turn on Idle Time Optimizer

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Optimizer** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

About the Norton Tasks

The **Norton Tasks** window provides an interface where you can view and monitor all Norton-specific background tasks. Norton 360 runs most of the background tasks when your computer is idle. The **Norton Tasks** window provides the details of the background tasks that Norton 360 performs.

The details include:

- The name of the Norton task

You can use the icon that appears before the name of a background job to start or stop a background task. You can start or stop a background task at any time.

- The timestamp of the Norton task

  You can view details such as the date on which the background job last ran and the time. These details help you decide whether to start a background task or wait for Norton 360 to run the job during idle time.
- The duration of the Norton task

  You can view the length of time that a Norton task ran the last time. The details also help you determine the length of time a background task takes to complete if you start it.
- The background task has run during idle time or not

  This detail helps you determine if a task has already run during idle time or you should run it.
- The status of the Norton task

  You can view details about the completion of the task.
- The power source that the Norton Task uses.

  You can specify the type of power source that each of the Norton Tasks uses. Use the **Configure** link that is available next to the power source icon to configure the power source for the Norton Tasks.

The Norton Tasks window lets you monitor the following Norton-specific tasks:

Automatic LiveUpdate	Automatic LiveUpdate automatically checks for definition updates and program updates when your computer is connected to the Internet. By default, Automatic LiveUpdate checks for updates every hour.
Backing up DefaultSet	Performs a backup of the files and data that are included in your backup set. If you created multiple backup sets, all of the backup sets appear on the Norton Tasks list. You can run a specific backup from the Norton Tasks window.
Disk Optimizer	Eliminates the file clutter and rearrange the placement of files on your computer disks to improve performance.
Full System Scan	Scans your entire computer for viruses, spyware, and different security vulnerabilities. It also runs other activities such as LiveUpdate, Cleanup, Disk Optimization, and Backup.
Insight Optimizer	Optimizes the boot volume of your computer.

Internet Explorer History Cleaner	Deletes the unnecessary Web page history that is left behind in your Internet browser's history folder. Removes the traces of any Internet searches that are performed on your PC.
Internet Explorer Temporary Files	Deletes the temporary files that are left behind on the hard disk after Internet browsing.
Norton Community Watch	Norton Community Watch protects your computer against potential risks. It collects the information about new security threats from your computer and submits the information to Symantec for analysis. Symantec assesses the data to identify the new threats and resolves it.

Norton Insight	Allows the smart scanning of files on your computer. It improves the performance of Norton 360 scans by letting you scan fewer files without compromising the security of your computer. Norton Insight lets you check the details of the Files of Interest that are available on your computer. You can view details such as signature of the file and the date on which the file was installed. You can also view details such as the trust level, community usage, resource usage, and the source of the file.
Pulse Updates	Pulse Updates check for definition updates every five minutes and downloads the streamed virus definitions. Pulse Updates provide the updates during the full updates, which LiveUpdate downloads automatically every few hours. Always ensure that the Pulse Updates option is turned on. It protects you from the latest threats without compromising your system performance or disrupting your online experience.

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. Quick Scan takes less time to scan than a Full System Scan because this scan does not scan your entire computer.
Windows Registry Cleaner	Deletes the inaccurate entries and obsolete entries in the Windows registry that can cause errors.
Windows Temporary File Cleaner	Deletes the unnecessary files that are left in Windows Temporary folders after a program is installed or updated.

The following grayed out categories of jobs run in the background to improve your system performance and protection. You can only view the last run details for the following activities.

Identity Safe Maintenance	Performs background maintenance tasks related to Identity Safe. Tasks include sending Identity Safe profile statistics and downloading the favorite icons.
AntiSpam Maintenance	Performs background maintenance tasks related to AntiSpam. Tasks include updating contacts and AntiSpam filters.

Licensing Maintenance	Performs background maintenance tasks related to licensing.
Insight Maintenance	Performs background maintenance tasks related to Norton Insight. Tasks include maintaining details about the stability and trust level of files in your computer.
Product Maintenance	Performs background maintenance tasks related to Norton 360. Tasks include clearing install logs and rescanning consolidated firewall rule.

You can also manually turn on Silent Mode for a specified duration.

Monitoring background jobs of Norton 360

The **Norton Tasks** window provides the details of the background tasks that Norton 360 performs and lets you view and monitor the background tasks. Norton 360 runs most of the background tasks when your computer is idle. Performing all background tasks when your computer is idle helps your computer to run at peak efficiency when you use your computer. However, you can manually start or stop a task at any time. You can also specify the **Idle Time Out** duration. After the **Idle Time Out** duration is reached, Norton 360 identifies the computer as idle and run the background tasks. You can use the **Idle Countdown** bar to confirm the idle state of your computer. You can also view the CPU graph and memory graph to obtain the performance data of your computer.

To monitor background jobs

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.
3. In the **Norton Tasks** window, view the details of background jobs.
4. Do one of the following:
   - To run a background job, click the play icon that appears before the name of the background job.
   - To stop a running background job, click the stop icon that appears before the name of the background job.
5. Click **Close**.

About Power Source

You can choose the power source for Norton 360 to perform the Norton Tasks when the computer is idle. Norton Tasks are background tasks that Norton 360 performs when your computer is idle. Norton Tasks include Quick Scan, Automatic LiveUpdate, Norton Community Watch, Norton Insight, Full System Scan, Insight Optimizer, and Pulse Updates. Norton 360 consumes more power when it runs Norton Tasks.

By default, Norton 360 performs these tasks only when your computer is connected to the external power. For example, if you are in an airport, and your computer is running on battery power, Norton 360 does not perform the Norton Tasks. In this way, you can extend the battery power of your computer. However, you can choose the power source for Norton 360 to perform the Norton Tasks.

You can select one of the following options:

External	Allows the Norton Tasks to run only when your computer uses external power. If you choose this option, Norton 360 performs the Norton Tasks when the computer is idle and connected to external power.
External and Battery	Allows the Norton Tasks to run irrespective if the computer uses external power or battery power. If you choose this option, Norton 360 performs the Norton Tasks when the computer is idle. It does not consider the type of power source the computer uses.

You can configure the power source for each of the Norton Tasks.

Configuring the Power Source

You can choose the power source for Norton 360 to perform the Norton Tasks when the computer is idle. Norton Tasks are background tasks that Norton 360 performs when your computer is idle.

By default, Norton 360 performs these tasks only when your computer is connected to the external power. You can configure the power source for each of the Norton Tasks.

To configure the power source

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, in the left pane, click **Norton Tasks**.

3. In the **Norton Tasks** window, under the **Power Source** column, click the **Configure** link for the Norton Task that you want to configure the power source.
4. In the **Power Source** window, select one of the following:
   - **External**

     Allows the Norton Task to run only when your computer uses external power.
   - **External and Battery**

     Allows the Norton Task to run irrespective if the computer uses external power or battery power.

     If you choose this option, Norton 360 performs the Norton Task when the computer is idle. It does not consider the type of power source the computer uses.
5. Click **OK**.
6. In the **Norton Tasks** window, click **Close**.

About Norton Insight

Norton Insight allows the smart scanning of files on your computer. It improves the performance of Norton 360 scans by letting you scan fewer files without compromising the security of your computer.

A Norton 360 scan can identify threats on your computer in the following ways:

The Blacklist technique	At regular intervals, Norton 360 obtains definition updates from Symantec. These updates contain signatures of known threats. Each time when Norton 360 obtains the definition updates, it performs a scan of all of the files that are available on your computer. It compares the signature of the files against the known threat signatures to identify threats on your computer.

The Whitelist technique	Norton 360 obtains specific information about the Files of Interest and submits the information to Symantec during idle time. The information includes things such as file name, file size, and hash key. Symantec analyzes the information of each File of Interest and its unique hash value and provides a confidence level to the file. The Symantec server stores the hash value and confidence level details of the Files of Interest. The server provides the details immediately after you open the **Norton Insight - Application Ratings** window. Even the slightest modification of the file causes a change in the hash value and the confidence level of the file. Typically, most Files of Interest belong to the operating system or known applications, and they never change. These files do not require repeated scanning or monitoring. For example, Excel.exe is a file that never changes but you always scan it during a normal security scan.

Symantec assigns the following confidence levels to Files of Interest:

Trusted	Symantec analyzes the file as trusted based on the statistical evaluation that is done on the files that are available within the Norton Community. If the file has three green bars, Symantec rates the file as **Norton Trusted**. The files that have three green bars display a Norton Trusted pop-up text when you move the mouse pointer over the green bars.
Good	Symantec analyzes the file as good based on the statistical evaluation that is done on the files that are available within the Norton Community. Symantec rates the trusted files as follows: ■ If the file has two green bars, Symantec rates the file as **Good**. ■ If the file has one green bar, Symantec rates the file as **Favorable**.
Unproven	Symantec does not have enough information about the file to assign a trust level to the file.
Poor	Symantec has only a few indications that the file is not trusted.

Norton 360 also provides different profiles to configure your scan performance. When you use the **Full Scan** profile, Norton 360 follows the Blacklist technique to scan your computer. It scans all of the files on your computer against the signatures that it obtained during definition updates. When you use the **Standard Trust** or **High Trust** profile, Norton 360 follows the Whitelist technique to scan the files based on their confidence level. This way, Norton 360 significantly reduces the time that is required to scan your computer completely for security threats.

The Whitelist technique that Norton Insight uses also helps in heuristic detection of suspicious applications. Normally, the execution behavior of well-known applications appears identical to the execution behavior of unknown applications. Such behavior results in false identification of good applications as suspicious, and therefore, necessitates security applications to maintain a low heuristic detection threshold. However, keeping a low detection threshold does not provide a complete heuristic protection against malicious applications. Norton 360 uses the Whitelist technique that helps maintain a high heuristic detection threshold. It excludes well-known applications from heuristic detection to prevent false detection of well-known applications and to ensure a high detection rate of malicious applications.

Viewing the files using Norton Insight

Norton Insight provides information about the Files of Interest that are available on your computer. Norton 360 lets you view specific categories of files based on the option that you select in the **Norton Insight - Application Ratings** window.

The drop-down list that is available in the **Norton Insight - Application Ratings** window provides you the following options:

All Running Processes	Lists the processes that run on your computer at that point in time when you selected this option.
All Files	Lists the Files of Interest.
Startup Items	Lists the programs that start when you start your computer.
All Loaded Modules	Lists all the files and programs that are currently loaded on to the program memory space.
Highest Performance Impact	Lists the programs that consume maximum resources of your computer. Norton 360 displays a list of top 10 resources that highly affect the performance of your computer.
Highest Community Usage	Lists the files that have the maximum community usage.

User Trusted Files	Lists the Files of Interest that you manually trusted in the **File Insight** window. This category does not list the files that do not belong to the File of Interest even if you manually trust the files. However, Norton 360 excludes all of the manually trusted files from Norton 360 scan when you configure **Scan Performance Profiles** to **High Trust**. You can also remove the user trust from all of the Files of Interest that you manually trusted. You can use the **Clear All User Trust** option next to the drop-down list to remove the user trust.
Untrusted Files	Lists the files that are not Norton Trusted. You can manually trust all the files that are not trusted by clicking the **Trust All Files** option next to the drop-down list.

You can view file details such as file name, trust level, community usage, resource usage, and the stability rating. There may be instances when the trust level of a file has changed or a process running might have stopped running. You can refresh the **Norton Insight - Application Ratings** window to update the file list and file details. The coverage meter provides a graphical representation of the percentage of the Norton Trusted Files and the total Files of Interest. The higher the percentage, the lesser time the scan takes.

To view the files using Norton Insight

1. In the Norton 360 main window, click **PC Security**, and then click **Run Norton Insight**.
2. In the **Norton Insight - Application Ratings** window, select an option from the **Show** drop-down list to view a category of files.
   You may need to scroll the window to view all the files that are listed in the details area.
3. Click **Close**.

To refresh the list of files

- In the **Norton Insight - Application Ratings** window, at the top of the file icon, click the refresh icon.

Checking the trust level of a file

Norton Insight lets you check the details of the Files of Interest that are available on your computer. You can view details such as signature of the file and the date on which the file was installed. You can also view details such as the trust level, stability details, community usage, resource usage, and the source of the file. You can use the **Locate** option to find the location of the file on your computer. When you right-click a file that is available on your computer, the shortcut menu displays **Norton 360** option and then **Norton File Insight** option. You can use the options to check the details of a File of Interest.

Norton 360 displays the **Norton File Insight** option only when you right-click a File of Interest. In Windows Safe mode, you cannot access this option for any file. Norton 360 also categorizes any file for which you open the **File Insight** window to view details as a File of Interest.

The Symantec server stores the hash value and trust level details of the File of Interest. The server provides the file details immediately after you open the **Norton Insight - Application Ratings** window. However, you can use the **Check Trust Now** option in the **File Insight**

window to update the trust value of a file. You can also manually trust any well-known files. You can change the trust level of any file to **User Trusted** other than the files that are Norton Trusted.

You can determine the resource usage of a file that is available on your computer. The **File Insight** window displays the CPU graph and the system resource usage details for the running processes. The graph shows the breakdown of overall system CPU usage and the CPU usage or memory usage by the process.

To check the trust level of a file

1. In the Norton 360 main window, click **PC Security**, and then click **Run Norton Insight**.
2. In the **Norton Insight - Application Ratings** window, click a file for which you want to check the details.
3. In the **File Insight** window, view the details of the file.
4. In the **File Insight** window, click **Close**.

To check the trust level of a specific file

1. In the Norton 360 main window, click **PC Security**, and then click **Run Norton Insight**.
2. In the **Norton Insight - Application Ratings** window, click **Check a Specific File**.
3. Browse to the location of the file for which you want to check the details.
4. Select the file, and then click **Open**.
5. In the **File Insight** window, view the details of the file.
6. In the **File Insight** window, click **Close**.

To find the location of the file

- In the **File Insight** window, click **Locate**.

To refresh the trust level of the file

- In the **File Insight** window, click **Check Trust Now**.

To manually trust the file

❖ In the **File Insight** window, in the **Details** tab, click **Trust Now**.
You can manually trust the files that are poor, unproven, or not Norton trusted.

To determine the resource usage of a running process

1 In the **File Insight** window, in the left pane, click **Activity**.
2 In the **Show** drop-down list, do one of the following:
- Select **Performance** to view the performance graph of the process.
- Select **Performance Alert** to view the performance alert-related details of the process.
- Select **Network** to view the network activities of the process.
- Select **Run Key change** to include registry changes.

Configuring the Scan Performance Profiles

The **Scan Performance Profiles** settings let you configure how Norton 360 should scan your computer based on the digital signature and confidence level of the files. To make Norton 360 scans lighter, faster, and more effective, you can exclude from scans the files that have known digital signatures or high confidence levels.

You can configure the **Scan Performance Profiles** settings to do the following:

- Configure to **Full Scan** to perform a complete scan of your computer.
  The complete scan includes a scan of all files on your computer irrespective of the confidence level or digital signature of the files.
- Configure to **Standard Trust** to perform a scan that excludes the files that are Norton Trusted.

Norton 360 scans the files that have a confidence level other than Norton Trusted.

- Configure to **High Trust** to perform a scan that excludes the files that have known digital signatures or high confidence levels.

  Norton 360 does not scan the files that have confidence level as Norton Trusted or User Trusted. It also excludes the Good files with high confidence level from the scan. It scans the files with confidence levels as Poor Trust, Unproven Trust, Bad Trust, and the files without a class 3 digital signature.

You must configure the **Scan Performance Profiles** settings before you run a scan or before a scan is scheduled to run. Norton 360 scans your computer according to the configuration you specified in the **Scan Performance Profiles** settings.

To configure Scan Performance Profiles from the Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
   On the **Scans and Risk** tab, in the **Scan Performance Profiles** row, click on one of the settings. Your options are:
   - **Full Scan**
   - **Standard Trust**
   - **High Trust**
3. Click **Apply**, and then click **Close**.

To configure Scan Performance Profiles from the Norton Insight - Application Ratings window

1. In the Norton 360 main window, click **PC Security**, and then click **Run Norton Insight**.

2 In the **Norton Insight - Application Ratings** window, move the **Scan Performance Profiles** slider to one of the settings. Your options are:
   - **Full Scan**
   - **Standard Trust**
   - **High Trust**
3 Click **Close**.

About Monthly Report

Monthly Report lets you view a summary of what Norton 360 has done for you. Norton 360 displays the monthly report every 30 days after you install your product. After 30 days of installation, Norton 360 displays the Monthly Report automatically. If you do not want Norton 360 to display the Monthly Report automatically, you can select the **Do not display monthly reports automatically** option in the **Norton Monthly Report** window.

You can view the Monthly Report using the **Check Monthly Report** option that is present in the **My Account** window.

Norton 360 lets you turn off or turn on Monthly Report from the **Administrative Settings** window. The **Norton Monthly Report** window displays the **Tip of the month** to recommend some of the product's features and services.

When your product expires after the trial period, Monthly Report displays the activation status of your product. However, when your product expires after the subscription period, Monthly Report displays the subscription status of your product.

Norton 360 provides reports based on the following categories:

PC Security	Lets you view the details of the various attacks your PC is protected from For example, you can view the total number of viruses and spyware from which you are protected.
Web	Lets you view the details of Antiphishing activities For example, you can view the total number of known authenticated sites that you visited.
Backup & Tuneup	Lets you view the details of Backup and PC Tuneup activities. For example, you can view the total number of files that you backed up on drive C of your computer. For example, you can view the total number of files that you backed up on drive C of your computer.

Monthly Report lets you view the latest news on Internet security and also provides information on how to stay safe while you are online. You can click the **Read More** option in the **Norton Monthly Report** window to view more information on how to stay safe online.

Viewing the Monthly Report

The Monthly Report lets you view how Norton 360 protected you for the past 30 days. This report includes different activities that Norton 360 performed to protect your computer.

The Monthly Report provides information about the following activities:

- The total number of threats that Norton 360 detected on your computer.
- The total number of phishing and authenticated Web sites that you visited.
- The total number of files that you backed up.
- The total number of unwanted files and the obsolete Windows registry entries that are removed.

If you do not want Norton 360 to display the Monthly Report automatically, you can do one of the following:

- Select the **Do not display monthly reports automatically** option in the **Norton Monthly Report** window.
- Turn off the **Monthly Report** option in the **Administrative Settings** window.

To view the Monthly Report

1. In the Norton 360 main window, click **Account**.
2. In the **My Account** window, click **Check Monthly Report**.
3. Click **Close**.

Maintaining total protection

3

This chapter includes the following topics:

- About total protection
- About keeping your computer secure
- About solving connection problems
- About responding to emergencies
- About monitoring protection features
- About viewing details of system vulnerabilities

About total protection

Norton 360 offers total protection of your PC that includes Antivirus and Spyware Protection, online identity theft protection, backup, and PC tuneup capabilities. It provides a complete protection against a wide range of threats, leaving you free to work and play confidently on your PC.

After you install Norton 360 and set up a backup storage destination, it then does all the rest. You do not have to do anything else to be protected. However, Norton 360 also lets you customize your firewall settings or adware protection, or set your own schedule for automatic activities.

Norton 360 is grouped into the following four categories of protection:

PC Security	Blocks and removes viruses and spyware from email and downloaded sites, protects against emerging threats, scans, cleans email attachments, and secures connections and data transmission between your computer and the Internet.
Identity Protection	Helps to guard against identity theft, verifies authenticity of Web sites.
Backup	Backs up all your important files and data to a variety of storage locations.
PC Tuneup	Finds and fixes common computer problems, cleans up unwanted cookies and files, and defragments the hard disk to optimize PC performance.

About keeping your computer secure

Norton 360 automatically protects your PC when you install it and updates itself regularly to maintain protection. However, you can increase the security of your PC further by learning how to avoid threats against your PC and your data.

To avoid email threats, do the following:

- Open only those email attachments that come from a trusted source and that you expect to receive.

- Delete all unwanted messages without opening them.
- Do not respond to email that you suspect is spam. Delete it.
- Be wary of any email that requests confidential information, and confirm the authenticity of the request before you reply.

To protect yourself from phishing attempts, do the following:

- When you visit a Web site, type the address directly into your browser rather than clicking a link.
- Provide personal information only on trusted sites. Examples include the sites that have "https" in the Web address or that have a lock icon at the bottom of the browser window.
- Do not provide personal information to any unsolicited requests for information.

To avoid viruses, worms, and Trojan horses, do the following:

- Transfer files to your PC only from a well-known source or a trusted source.
- Do not send or receive files over instant messaging connections.
- Terminate an instant messaging connection if a person on your buddy list sends strange messages, files, or Web links.

To avoid spyware, do the following:

- Do not approve suspicious error messages from within your Web browser.
- Be suspicious of "free deal" offers because spyware may come as part of such a deal.
- Carefully read the End User License Agreement for the programs that you install. Also, do not install a program if other programs are installed as part of the required program.

About solving connection problems

Norton 360 uses an Internet connection to support several of its protection features. If you use a proxy server to connect to the Internet, you must configure the proxy settings of Norton 360. You can configure Network Proxy Settings in the **Administrative Settings** window.

If you cannot connect to the Internet after you install Norton 360, you can use the Support features to help you troubleshoot your connection problem.

About responding to emergencies

Norton 360 automatically downloads definition updates regularly and secures your computer from latest viruses and unknown threats. In addition, Norton 360 monitors your Internet activities to protect your computer from the Internet-based threats that exploit software vulnerabilities.

However, security issues can arise, and you need to decide which action to take.

If you think that your computer is infected with a virus or with destructive software, you can take the following actions:

Quick Scan	Helps you to scan the possible virus-infected areas of a computer that the viruses and other security risks often target Because this scan does not scan your entire computer, it takes lesser time to run than a Full System Scan.

Full System Scan	Checks all boot records, files, and running programs to protect your computer from viruses and spyware It also runs other tasks (such as LiveUpdate, Registry Cleanup, Disk Optimization, and Backup) to provide a high level of protection and improve the performance of your computer. Consequently, when you run a Full System Scan with administrator privileges, it scans more files than when you run it without administrator privileges. This scan might take more time than the other scans.
Custom Scan	Scans a specific file, folder, drive, or removable drive that you choose. You can also create your own scan and schedule it to run at a specific time.
Custom Task	Checks for vulnerabilities and risks, and protects your computer by running the following checks: **LiveUpdate** **Internet Explorer Temporary Files** **Windows Temporary Files** **Internet Explorer History** **Disk Optimization** **Registry Cleanup** **Backup**

When you right-click a folder, the shortcut menu displays Norton 360 and then **Scan Now** option. You can use this command to scan any particular folder.

When you right-click a file, the shortcut menu displays Norton 360 and then **Insight Network Scan** option. You can use this command to scan a file using both local definitions and definitions that are hosted in the Cloud.

About monitoring protection features

Your Symantec product maintains records of all protection-related actions that it takes and the activities that it monitors. You can review the history and the logs through Security History. You can view summary and results of activities and scans. You can also monitor other security tasks.

About Security History

Security History window lets you do the following:

- View the summary of alerts and event messages.
- View the results of scans that are run on your computer.
- View the items that you submitted to Symantec Security Response Web site.
- Manage Quarantine items.
- Monitor the security tasks that your products perform in the background.

Security History lets you monitor the security tasks that your product performs in the background. In addition, the alerts that you receive can be reviewed at any time in Security History. If you cannot review an alert when you receive it, you can review it later in Security History.

The alerts, scan results, and other security items that are related to various product features appear under their respective categories in the **Security History**

window. For example, the security items that are related to the Quarantine feature appear under the **Quarantine** category. In addition, the **Security History** window displays details of each item in the **Details** pane.

Based on their functionalities, Security History broadly organizes all categories into the following groups:

- **All Activity**
- **Protection and Performance**
- **Submissions and Errors**
- **PC Tuneup**
- **Informational**

By default, the following information categories are available in the **Security History** window:

- **Recent History**
- **Full History**
- **Scan Results**
- **Resolved Security Risks**
- **Unresolved Security Risks**
- **Quarantine**
- **SONAR Activity**
- **Firewall – Network and Connections**
- **Firewall – Activities**
- **Intrusion Prevention**
- **Download Insight**
- **AntiSpam**
- **Identity**
- **Norton Product Tamper Protection**
- **Performance Alert**
- **Metered Network**
- **Backup**
- **Sites reported to Symantec**
- **Norton Error Reporting**

- **Email Errors**
- **Norton Community Watch**
- **Registry Cleanup**
- **File Cleanup**
- **Disk Optimization**
- **Silent Mode**
- **LiveUpdate**

You can view the security items based on the category of events that you select and the search string that you provide. Norton 360 restricts the number of search results that appear on each page in the **Security History** window. Therefore, Security History divides the items that are returned for any search criteria and displays them on separate pages. You can use the pagination scroll at the bottom of the window to navigate to different pages sequentially. In case you want to view a specific page, you can use the **Go to page** option to open the page. The maximum number of items that appear per page is 100.

Based on the security status of an item in an information category, you can take an appropriate action to resolve a risk or a threat. The actions that you can perform include the following:

- Restore and exclude a quarantined item.
- Remove an item from Security History.
- Submit an item to Symantec for further analysis.
- Trust or restrict devices on a selected network.
- Remove the trusted or restricted status of devices on the selected network.
- Allow a selected program to access the Internet.
- Configure Norton 360 to notify you when it blocks a selected attack signature.

Norton 360 also lets you save the security events history. You can view the security event information whenever you want. If you want to analyze the security events for a particular day, you can save the Security

History logs for that day. You can later import the file into Security History and analyze the data.

Viewing items in Security History

Security History provides a record of all the activities that Norton 360 performed on your computer.

You can view details about all the activities including:

- Security History alerts and event messages
- Results of different scans
- Information that you submitted to Symantec Security Response Web site
- Quarantined items
- Norton 360 firewall activities
- Norton 360 PC Tuneup activities
- Norton 360 backup and restore activities
- Security tasks that Norton 360 performed in the background

Based on their functionalities, all Security History categories appear under the following groups in the **Show** drop-down list:

- **All Activity**
- **Protection and Performance**
- **Submissions and Errors**
- **PC Tuneup**
- **Informational**

The items that are related to the various product features appear under their respective categories in the **Security History** window. For example, the security items that are related to the Quarantine feature appear under **Quarantine** category in the **Security History** window. In addition, the **Security History** window displays details of each item in the **Details** pane.

To view items in Security History

1 In the Norton 360 main window, click **Tasks**.

2 In the **Tasks** window, under **General Tasks**, click **Check Security History**.

3 In **Security History** window, in the **Show** drop-down list, select the category of items that you want to view. Your options are:

Recent History	The **Recent History** view in the **Security History** window displays the alerts that you received during the last seven days. It lists the history of certain recent security events.
Full History	The **Full History** view in the **Security History** window displays the complete Security History.
Scan Results	You can scan your computer to check if any virus, spyware, malware, or security risk has infected your computer. The **Scan Results** view in the **Security History** window displays the details about the scans that are run on your computer.

Resolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Resolved Security Risks** view in the **Security History** window displays a list of security risks that Norton 360 has detected and then repaired, quarantined, or removed. The quarantined items are listed in the **Quarantine** view. You can also view the quarantined items in the **Quarantine** view.
Unresolved Security Risks	The security risks include the suspicious programs that can compromise the security of your computer. The **Unresolved Security Risks** view in the **Security History** window displays a list of security risks that Norton 360 was not able to repair, remove, or quarantine. Certain threats require system restart, logs for such threats can be cleared only after you restart your system.

Quarantine	The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide an action to take on them. The **Quarantine** view in the **Security History** window displays all of the security risks that are isolated in the Security History Quarantine.
SONAR Activity	Symantec Online Network for Advanced Response (SONAR) identifies new threats based on the suspicious behavior of applications. SONAR detects and protects your computer against malicious code even before virus definitions are available through LiveUpdate. The **SONAR Activity** view in the **Security History** window displays details about the security risks that SONAR detects. This category also lists any activity that modifies the configuration or the settings of your computer. The **More Details** option for this category provides details about the resources that this activity affects.

Firewall - Network and Connections	The firewall monitors the communications between your computer and other computers on the Internet. The **Firewall - Network and Connections** category in the **Security History** window displays information about the networks that your computer connects to. It also displays the actions that you have taken to trust or to restrict networks and computers. This category also displays a history of all of the TCP/IP network connections that were made with your computer. Network connections are logged when the connection is closed. The **Security History - Advanced Details** window for this category lets you modify trust or restrict settings for computers and networks.

Firewall - Activities	The firewall monitors the communications between your computer and other computers on the Internet. The firewall maintains rules to control Internet access to and from your computer. The **Firewall - Activities** view in the **Security History** window displays the rules that firewall creates. The rules that you create also appear in this view. The **Security History - Advanced Details** window for this category shows the created Program rules. It also lets you allow a blocked program rule.
Intrusion Prevention	Intrusion Prevention scans all the network traffic that enters and exits your computer for known threats. The **Intrusion Prevention** view in the **Security History** window displays details about recent Intrusion Prevention activities. The **Security History - Advanced Details** window for this category lets you control whether or not to be notified when Intrusion Prevention detects an **Intrusion Prevention** signature.

Download Insight	Download Insight processes any executable file that you download for analysis of its reputation level. It then informs you about the processing results based on the Download Insight settings. The **Download Insight** view in the **Security History** window displays details of all events that Download Insight processes and notifies. This view also contains information about the actions that you take based on the reputation data of the events.
AntiSpam	Norton AntiSpam protects your computer from exposure to unsolicited email. The **AntiSpam** view in the **Security History** window displays details about the email messages that AntiSpam has processed.
Identity	The various features of Identity Safe help you manage your identities and provide additional security while you perform online transactions. The **Identity** view in the **Security History** window displays the Antiphishing definitions that Norton 360 downloads when you run LiveUpdate to obtain the latest virus definitions.

Norton Product Tamper Protection	Norton Product Tamper Protection lets you protect your Norton product from any attack or modification by unknown, suspicious, or malicious applications. The **Norton Product Tamper Protection** view in the **Security History** window displays details about unauthorized attempts to modify Symantec processes. The tasks that your Symantec product blocks also appear in the list.
Performance Alert	The performance alert feature lets you view, monitor, and analyze the impact of the system activities on your computer. The **Performance Alert** view in the **Security History** window provides details about the impact of the processes that run on your computer. The details include the process name, the resources used, the extent of resource utilization, and the overall impact of the process on your computer. In addition, logs related to performance alerts and the programs that you have excluded from performance alerts also appear in the list.

Metered Network	Metered Broadband Mode lets you set up policies and restrict the Internet usage of Norton 360. You can define the amount of network bandwidth that Norton 360 can use. The Metered Network view in the Security History window provides details about the actions that you performed to restrict the Internet usage of Norton 360.
Backup	The **Backup** view displays the list of the backup and restore activities that you performed.
Sites reported to Symantec	In some cases, you might have submitted evaluation of certain Web pages to Symantec. The **Sites Reported to Symantec** view in the **Security History** window displays all the Web sites that you reported to Symantec to verify authenticity.

Email Errors	Email errors include any failure that occurs when Norton 360 tries to send, download, or scan an email message that you send or receive. The **Email Errors** view in the Security History displays details about any Email Error alerts that you receive when an Email error occurs. Details include the **Error ID** and the **Error message**. This view also displays information about subject, sender address, and the recipient address that are related to the email message in the alert.
Norton Community Watch	The Norton Community Watch feature lets you submit any suspicious security or suspicious application data to Symantec for analysis. Symantec assesses the data to determine the new threats. The **Norton Community Watch** view in the **Security History** window displays a list of files that you have submitted to Symantec for analysis. Files, at various stages of submission, also appear in the list.

Registry Cleanup	The windows registry can contain the entries that refer to files that do not exist. Such broken registry items can slow down your computer. Registry Cleanup scans your computer and cleans any broken registry entries that it finds. The **Registry Cleanup** view in the **Security History** window displays the list of the Registry Cleanup activities that been performed in your computer.
File Cleanup	The File Cleanup feature removes unwanted temporary files including leftover Internet browser files, Internet search words, and other temporary files. The **File Cleanup** view in the **Security History** window shows the list of the File Cleanup activities that were performed on your computer.
Disk Optimization	Disk optimization is a process in which the physical locations of files are streamlined. Files and metadata are re-arranged to improve data access time. The disk optimization view in the **Security History** window shows the list of the disk optimization activities that were performed on your computer.

Silent Mode	Silent Mode suppresses alerts and notifications and temporarily suspends most of the background activities. The **Silent Mode** view in the **Security History** window displays the summary of the Silent Mode sessions. The summary includes the following information: ■ The type of Silent Mode such as Silent Mode or Quiet Mode ■ The type of program that turns on Silent Mode such as disk burning or TV recording ■ The name of User-Specified program that turns on Silent Mode ■ Whether Silent Mode is turned on or turned off
LiveUpdate	LiveUpdate obtains the latest virus definition updates and the program updates to all the Symantec products that you installed on your computer. These updates protect your computer from newly discovered threats. The **LiveUpdate** view in the **Security History** window shows the details of the LiveUpdate activities on your computer. The details include the severity, the status, and the duration of the LiveUpdate sessions on your computer.

4 Click a row to view details for that item.
If you want to view additional information about an item, click the **More Details** option in the **Details** pane or double-click the particular row. You can view the advanced details about the item in the **Security History-Advanced Details** window and take actions as needed. For some categories, the **More Details** option opens the **File Insight** window that displays the details about the selected Security History event. You must use the **Options** link in the **Security History** window to select an action that Norton 360 must perform on any item in these categories. The **Options** link is also available in the **File Insight** window for certain items.

About the Security History - Advanced Details window

The **Security History - Advanced Details** window lets you view more information about the items that you select in the **Show** drop-down list in the **Security History** window. You can also perform any action that is available for the selected item from this window.

The following table lists the categories that provide the advanced details about the Security History items:

Alert Summary	Displays the following information about the item: ▪ **Severity** This category displays the risk level of the selected item. The various levels of security risks are **High**, **Medium**, **Low**, and **Info**. ▪ **Activity** This category displays the activity that was performed by Norton 360. ▪ **Date & Time** This category displays the date and time of the activity. ▪ **Status** This category displays the status of the action that has been taken on the item. ▪ **Recommended Action** This category displays the actions that you might need to perform.
Advanced Details	Displays the detailed information of the item You can view the details such as category, risk level, risk category, submission date of the risk, risk status, risk description, and recommended actions for the items.

Actions	

	Displays the actions that are available for the selected item The options in the **Actions** view vary depending on the options that are available in the **Show** drop-down list in the **Security History** window. The following are some of the **Actions** options: **Trust** This action allows access to or from the selected computer or all of the unclassified computers on the selected network. This option is available in the **Security History - Firewall - Network and Connections** view. **Restrict** This action blocks access to or from the selected computer or all of the unclassified computers on the selected network. This option is available in the **Security History - Firewall - Network and Connections** view. **Remove trust** Removes the trusted status from the selected computer or from all of the unclassified computers on the selected network. This option is available in the **Security History - Firewall - Network and Connections** view. **Remove restriction**

	This action removes the restricted status from the selected computer or from all of the unclassified computers on the selected network. This option is available in the **Security History - Firewall - Network and Connections** view. **View Rule** This action shows the firewall rule that is used to control the Internet access attempts by the selected program in the **Program Control** window of Norton 360. This option is available in the **Security History - Firewall-Activities** view. **Allow** This action allows the selected program to access the Internet. This option is available in the **Security History - Intrusion Prevention** view. **Stop Notifying Me** This action prevents Norton 360 from notifying you when it blocks the selected attack signature in the future. This option is available in the **Security History - Intrusion Prevention** view.

	▪ **Notify Me** This action allows Norton 360 to notify you when it blocks the selected attack signature in the future. This option is available in the **Security History - Intrusion Prevention** view.
Risk Management	Displays the links that provide the information that is related to the selected item For some Security History items, this view lets you access the relevant settings pane of the Norton 360 window.

About the File Insight window

The **File Insight** window provides details about any File of Interest that is available on your computer. This option of file analysis is available for the files that you download, scan, or use to perform an activity.

You can access the **File Insight** window in different ways. For example, you can use the various notifications, alerts, scan and performance-related windows, and the shortcut menu of the various files that are present on your computer to open the window. Security History provides a centralized location where you can access the **File Insight** windows of the various events that are related to Security Risks, Download Insight, and Performance.

The File Insight window lets you view more details of events that belong to some of the following categories in the **Security History** window:

Resolved Security Risks	Lets you view the detailed information about the resolved security risks in an organized way. The **Resolved Security Risks** category includes the infected files that Norton 360 repairs, removes, or quarantines. This category mostly includes the medium-level or the high-level risks that are either quarantined or blocked. The **File Insight** window provides details about the risk level, the origin, and the activity report of the resolved security risks on your system.
Unresolved Security Risks	Lets you view the detailed information about the unresolved security risks in an organized way. The **Unresolved Security Risks** category includes the infected files for which Norton 360 was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of the unresolved security risks on your system.

Quarantine	Lets you view the detailed information about quarantined security risks in an organized way. The **Quarantine** category includes the infected files that are isolated from the rest of your computer while they await your attention for a suitable action. The **File Insight** window provides details about the risk level, the origin, and the activity report of quarantined security risks on your system.
Download Insight	Lets you view the reputation details of a file that you download. You can use these details to determine the safety level of the file and then decide the action that you want to perform.
Performance Alert	Lets you view the performance details of any File of Interest that is available on your computer. The information includes the general details, the origin and lineage information, the resource usage, and the actions that the file has performed on your system.

The **File Insight** window provides various details about the Security History item. These details are classified in different tabs in the **File Insight** window.

You can select a tab to view more details about it. The **File Insight** window provides details about a file in the following tabs:

Details	Displays the information such as the confidence level, community usage of a file, how long ago the file was released and how stable the file is. Stability ratings of a file may vary depending upon your operating system. You can view details such as the signature and the date on which the file was created. You can determine if a file is a startup file and the date on which the file was last used.
Origin	Provides the lineage details of a file. You can view the file name and the URL of the source from where the file was downloaded. The lineage details of a file are available only if you downloaded or created the file after you installed Norton 360. If the historical details of a file are not available, Norton 360 disables this **Origin** section.

Activity	Provides the details about the suspicious actions performed by the file on your computer. It also provides information about the resource usage of a process and the effect of the process on the overall CPU utilization of your computer.

Based on the severity of the security risks and the risk type, Norton 360 might display one or more of the following options in the **File Insight** window:

Locate	Lets you locate the file on your computer. This option is available at the top of the window.
Copy to Clipboard	Lets you copy the data from the **File Insight** window to the clipboard. After you copy the content to the Clipboard, you can open a document, paste the data, and save the document.
Options	Lets you access the **Threat Detected** window and view more details and perform actions.
Learn More	Lets you access the online tutorial page to get more information about the file.

About the Threat Detected window

The **Threat Detected** window appears whenever Norton 360 detects a security risk on your computer. You can use this window to view details about the risk and select an action for the risk. Sometimes, you may want to access the **Threat Detected** window for the same risk again. In that case, the window can be opened at any time from Security History. Security History is the centralized location where you can access the **Threat Detected** windows of risks that belong to some of the following categories:

Resolved Security Risks	This category includes the security risks or the infected files that Norton 360 has detected and then repaired, quarantined, or removed.
Unresolved Security Risks	This category includes the security risks or the infected files that Norton 360 was not able to repair, remove, or quarantine.
Quarantine	This category includes the security risk items that are isolated from the rest of your computer while they await your attention for a suitable action.

The action options in the **Threat Detected** window for a risk vary depending on the risk type and its severity level. The following are some of the options that are available in this window:

Restore	Returns the security risk that is quarantined to the original location on your computer

	Returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans
Remove this file	Removes the security risk from your computer and quarantines it
Exclude this program	Excludes the security risk from future scan
Remove from history	Removes the selected security risk item from the Security History log
Get help	Takes you to the Symantec Security Response Web site
Submit to Symantec	Sends the security risk to Symantec

Searching in Security History

You can search the items that are listed in Security History. You can use the **Quick Search** option to find items using a keyword or the name of a security risk. If you want to view all of the Security History items that pertain to a particular security risk, you can filter the items using **Quick Search**. For example, if you want to view all of the alerts that Auto-Protect has generated, you can type Auto-Protect and filter the list.

You can clear the search results and return to the current Security History list by clicking the black cross (x) icon in the **Quick Search** box.

The **Quick Search** option works on the current view only. If you want your search to include all of the items

in Security History, you must select the **Full History** view.

To search in Security History

1. In the **Security History** window, in the **Quick Search** text box, type the name of the item that you want to search.
2. Click **Go**.

Exporting or Importing Security History information

Norton 360 lets you export the Security History events to a file. You can export and save the Security History events and view them at your leisure.

For example, you can analyze the security events on a particular day. You can use the **Quick Search** option to obtain a list of all of the items that are related to a particular security risk. You can then use the **Export** option to save the list in the Security History log. You can later import the log file and analyze the data.

Security History stores the information in a separate file. When the file size reaches its maximum size limit, information that is related to new events overwrites the information that is related to older events. You can export the log periodically, if you want to keep the entire Security History information.

You can save your log file in one of the following file formats:

- Security History Log Files (.mcf)

  The .mcf file format is the Security History Log Files format and is proprietary to Symantec.

  When you use this file type option, you can view the file only in the **Security History** window.
- Text Files (.txt)

  The data is saved in a comma-separated text format.

  When you use this file type option, you can open and view the file externally without using Security History.

You can import only the log files that have .mcf file extension. When you import a log file, the exported list of Security History information in the log file appears. This list replaces the current security events list. You can select an option in the **Show** drop-down list to view the option-specific details that are saved in the log file. To revert to the current Security History list you must click the **Close file: *file_name*.mcf** link.

To export Security History information

1. In the Norton 360 main window, click **Tasks**.
2. In the **Tasks** window, under **General Tasks**, click **Check Security History**.
3. In the **Security History** window, in the **Show** drop-down list, select an option.
4. Click **Export**.
5. In the **Save As** dialog box that appears, navigate to a location and specify the name for the file.
   The category name in the **Show** drop-down list appears as the default file name. You can provide a file name of your choice.
6. In the **Save as type** box, select the format in which you want to save your log file.
7. Click **Save**.

To import Security History information

1. In the Norton 360 main window, click **Tasks**.
2. In the **Tasks** window, under **General Tasks**, click **Check Security History**.
3. In the **Security History** window, click **Import**.
4. In the **Open** dialog box that appears, browse to the folder that has the file you want to import.

5 Select the .mcf file and click **Open**.
You can only open log files of .mcf format in the **Security History** window. You can open and view log files of .txt file externally without using Security History.
In the import mode, you cannot make modifications to the information. For example, you cannot clear the logs. You can revert to the current Security History list by closing the file.

Managing items in the Quarantine

The Security History Quarantine provides a safe location on your computer where you can isolate items while you decide on an action to take on them. Quarantined items are isolated from the rest of your computer so that they cannot spread or reinfect your computer. In some cases, you may have an item that you think is infected, but is not identified as a risk by the Norton 360 scans. You can manually place such items in the Quarantine.

You cannot open quarantined items accidentally and spread the virus, but you can evaluate the quarantined items for possible submission to Symantec.

The Security History Quarantine includes the following groups of items:

Security risks	Includes the items such as spyware and adware that are generally low risk and that another program requires to function properly. You can restore these items if necessary.
Security threats	Includes viruses and other high-risk items.

Once an item has been quarantined, you have several options. All of the actions that you take on quarantined items must be performed in the Security History Quarantine.

To perform an action on a quarantined item

1. In the **Security History** window, in the **Quarantine** view, select the item on which you want to perform the action.
2. In the **Details** pane, click **Restore & Options**.
   You can use the **More Details** link to view more details about the item before you select an action for it. The link opens the **File Insight** window that contains more information about the risk.

3 In the **Threat Detected** window, select the action that you want to perform. Some of the options are:

Restore	Returns the security risk that is quarantined to the original location on your computer This option is available only for the detected viral threats.
Restore & exclude this file	Returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans This option is available for the detected viral and non-viral threats.
Remove from history	Removes the selected item from the Security History log
Submit to Symantec	Sends the selected item to Symantec for evaluation of the security risk In some cases, Norton 360 might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can use this option to submit the item to Symantec for further analysis.

You can also navigate to this window by using the **Options** link in the **File Insight** window for some risks.

4 Follow the on-screen instructions.

Adding an item to the Quarantine

Security History Quarantine provides a safe location on your computer in which you can isolate items while you decide on an action to take on each item.

The **Quarantine** view in the **Security History** window displays a list of quarantined items. You can view the name and the risk status of each quarantined item.

You can manually add an item to the Security History Quarantine. You can use the **Add to Quarantine** option in the **Quarantine** view in the **Security History** window to quarantine the items that you suspect are infected. This action has no effect on the items that are already quarantined.

You cannot add a known Good File to Quarantine.

To add an item to the Quarantine

1. In the **Security History** window, in the **Quarantine** view, click **Add to Quarantine**.
2. In the **Manual Quarantine** dialog box, in the **Description** text box, type a short name for the item that you want to add.
   This text appears in the Quarantine, so you should use a recognizable description.
3. Click **Browse**.
4. In the **Select File to Quarantine** dialog box, browse to the item that you want to add, select it, and then click **Open**.
5. Click **Add**.
6. Click **Close**.

Restoring an item from the Quarantine

Some programs rely on other programs that are classified as security risks to function. The program may not function if a particular security file is removed. All of the removed security risks are automatically backed up in the Security History Quarantine. This way, Norton 360 lets you restore any risk to regain the

functionality of a program that requires the risk program to run.

For example, a shareware or freeware program that you download may use adware to keep its price low. In this case, you can allow the security risk program to remain on your computer or restore it if Spyware Protection has removed it.

Some quarantined items are successfully disinfected after Norton 360 rescans them. You can also restore such items.

If you restore an item to a directory other than its original location, it may not function properly. Therefore, it is recommended that you reinstall the program.

To restore an item from the Quarantine

1. In the **Security History** window, in the **Quarantine** view, select the item that you want to restore.
2. In the **Details** pane, click **Restore & Options**.
3. In the **Threat Detected** window, click **Restore & exclude this file**.
   This option returns the selected Quarantine item to its original location without repairing it and excludes the item from being detected in the future scans.
4. In the **Quarantine Restore** window, click **Yes**.
   In case of non-viral threats, you can use the option that is available in this window to exclude the security risk. Norton 360 does not detect the security risks that you exclude in the future scans.
5. In the **Browse for Folder** dialog, select the folder or drive where you want to restore the file and then click **OK**.
6. Click **Close**.

Removing an item from the Quarantine

You can configure Norton 360 to remove a security risk from your computer. You can use the **Restore** option

to remove the security risk and places it in the Security History Quarantine. Some programs may rely on the security risk item that you quarantine to function. In this case, you can restore the security risk to regain the functionality of a program that requires the risk program to run.

The **Restore** option is only available for the security risks that are manually quarantined.

To remove an item from the Quarantine

1. In the **Security History** window, in the **Quarantine** view, select the item that you want to remove.
2. Click **Restore & Options**.
3. In the **Threat Detected** window, click **Restore**. This option is available for the security risks that are manually quarantined.
4. In the **Quarantine Restore** window, click **Yes**.
5. Click **Close**.

Manually submitting an item to Symantec

When a virus or other risk is detected, it is automatically submitted to Symantec Security Response Web site for analysis. If you have turned off the option to submit risks automatically, you can manually submit them from the Security History Quarantine. You must have an Internet connection to submit an item.

When you submit files to Symantec automatically or manually, you contribute to the effectiveness of your Symantec product. For example, you can submit an item that has not been detected during scanning that you believe may be a security risk. Symantec Security Response analyzes the file. If it is identified as a security risk, it is added to a future definition update.

Personally identifiable information is never included in submissions.

In some cases it is necessary for Symantec Security Response to block submissions of a particular type or

volume. These items appear as **Not Submitted** in Security History.

To manually submit an item to Symantec

1. In the **Security History** window, in the **Quarantine** view, select the item that you want to submit to Symantec.
2. In the **Details** pane, click **Restore & Options**.
3. In the **Threat Detected** window, click **Submit to Symantec**.
4. In the dialog box that appears, click **OK**.

About viewing details of system vulnerabilities

The **Intrusion Prevention** feature of Norton 360 provides a proactive solution to prevent the threats that might exploit the vulnerabilities of the programs or the operating system of your computer. Norton 360 now provides the **Vulnerability Protection** feature that enables you to view details of the protection feature against possible attacks on these vulnerabilities. **Vulnerability Protection** displays an extensive list of the programs on your computer that contain vulnerabilities. In addition, it provides details about the vulnerability and the solution that **Intrusion Prevention** provides to identify any attack on the vulnerability. You can use **Vulnerability Protection** to view the correlation between the vulnerabilities that your computer is protected against and the programs that may contain these vulnerabilities.

About Vulnerability Protection

Vulnerability Protection is a component of Intrusion Prevention System. Vulnerability Protection provides information about the susceptibility of the programs that may be on your computer against malicious

attacks. It also provides information about the known attacks that they are protected from.

Vulnerabilities are flaws in your programs or your operating system that can create weaknesses in overall security of your system. Improper computer configurations or security configurations also create vulnerabilities. External attackers exploit these vulnerabilities and perform malicious actions on your computer. Examples of such malicious attacks are active desktop monitoring, keylogging, and hacking. Such attacks can slow down the performance of your computer, cause program failure, or expose your personal data and confidential information to the hackers.

Norton 360 provides the signature-based solutions to protect your computer from the most common Internet attacks. Attack signatures contain the information that identifies an attacker's attempt to exploit a known vulnerability in your operating system or your computer programs. The Intrusion Prevention feature of Norton 360 uses an extensive list of attack signatures to detect and block suspicious network activity.

Vulnerability Protection lets you view the correlation between the vulnerabilities that your computer is protected against and the programs that may contain these vulnerabilities. For example, if Internet Explorer does not handle certain HTTP responses, it can result in a vulnerability that can be exploited. In this case, Vulnerability Protection lists Internet Explorer as a vulnerable program. It also provides details about the signatures that Intrusion Prevention uses to detect any attempt to exploit this vulnerability.

Viewing the list of vulnerable programs

The **Vulnerability Protection** window lets you view the extensive list of programs with the known vulnerabilities that Norton 360 protects you against.

For each program, you can view details such as the name of the program, its vendor, and the number of

vulnerabilities that the program contains. You can also view more details about the vulnerabilities by clicking on the program name.

To view the list of vulnerable programs

1. In the Norton 360 main window, click **Tasks**.
2. In the **Tasks** window, under **General Tasks**, click **Check Vulnerability Protection**.
3. After you finish viewing the list, click **Close**.

Viewing details about a vulnerable application

The **Vulnerability Protection** window displays the list of the programs on your computer that are susceptible to malicious attacks. In addition, you can view details of the vulnerabilities that a program contains. The **Program Vulnerability Details** window displays the names of the attack signatures that Intrusion Prevention uses to detect any attempts to exploit the vulnerabilities in the program.

You can click an attack signature to get additional information about the signature in the Symantec Security Response Web site.

The **Intrusion Signatures** window of **Intrusion Prevention** lets you view a list of attack signatures. Intrusion Prevention relies on this list of attack signatures to detect and block suspicious activity. You can uncheck a signature from the list, if you do not want Norton 360 to monitor the signature. The **Program Vulnerability Details** list does not include any signature that you disable in the **Intrusion Signatures** window. By default, all the signatures in the **Intrusion Signatures** window are turned on. Unless you have a good reason to disable a signature, you should leave the signatures turned on. If you disable a signature, your computer may be vulnerable to attack.

To view details about a vulnerable application

1. In the Norton 360 main window, click **Tasks**.

2 In the **Tasks** window, under **General Tasks**, click **Check Vulnerability Protection**.
3 In the **Vulnerability Protection** window, in the **Program** column, click the program name for which you want to view the details.
4 In the **Program Vulnerability Details** window, view the signature details of the program.
5 If you want to view additional information about the signature, then click the signature name.
6 After you finish viewing the vulnerability details, in the **Program Vulnerability Details** window, click **Close**.
7 In the **Vulnerability Protection** window, click **Close**.

Scanning your computer

4

This chapter includes the following topics:

- About the Norton 360 scans
- About Computer Scan
- About Insight Network scan
- About Reputation Scan
- About Scan Facebook Wall
- About SONAR Protection
- About scanning Office documents
- About Silent Mode
- About boot time protection
- Running a scan at the command prompt

About the Norton 360 scans

Norton 360 scans secure your computer from all types of viruses and unknown threats using the latest virus definitions. It also scans all the Internet activities that are performed on your computer to protect your computer from the Internet-based threats that exploit software vulnerabilities.

Norton 360 automatically performs different types of scans to secure your computer from latest threats. It also lets you run different types of scans manually to secure your computer.

By using Norton 360, you can run the following types of scans:

Computer Scan	**Computer Scan** uses the latest virus definitions that are available locally in the computer. If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer. The three types of scans that are available under **Computer Scan** are **Quick Scan**, **Full System Scan**, and **Custom Scan**.
Insight Network Scan	**Insight Network Scan** uses the virus definitions that are available locally and hosted in the Cloud. **Insight Network Scan** detects the files that are suspicious or vulnerable on your computer using the reputation-based threat detection. Norton 360 performs an **Insight Network Scan** only when the **Insight Protection** option is turned on. By default, the **Insight Protection** option is turned on. You can see this **Insight Protection** option under **Scans and Risks** tab in the **Antivirus** settings window.

Reputation Scan	**Reputation Scan** displays the reputation information of the files on your computer. It displays the reputation information such as trust level, prevalence, stability rating, and resource usage. **Reputation Scan** displays the detailed reputation information of the good files and the number of bad files that have been detected or removed. **Reputation Scan** also internally performs **Computer Scan** and **Insight Network Scan** to detect the threats. The different types of scans that are available under Reputation Scan are **Quick Scan**, **Full System Scan**, and **Custom Scan**. Norton 360 Reputation Scan is applicable only for the executable files and the installer files.

Scan Facebook Wall	**Scan Facebook Wall** lets you scan the links and URLs that are available on your Facebook profile. When you click the **Scan Facebook Wall** option, Norton 360 takes you to the Facebook login Web page. After you log in to your Facebook profile, Norton Safe Web asks you to grant permission to access your Facebook wall. To do so, use the **grant us permission to access your stream** option available on the Facebook Web page, and then follow the on-screen instructions. After you grant permission, Norton safe Web scans all the available links on your Facebook wall each time you use **Scan Facebook Wall** option. It then displays the security status of the scanned URLs.

Norton 360 keeps your computer secure from latest threats by automatically running Full System Scan when your computer is in the idle state.

About Computer Scan

Norton 360 automatically downloads latest virus definition regularly and secures your computer from all types of viruses and unknown threats. When Norton 360 performs a Computer Scan, it uses the latest virus definitions that Symantec provides.

The threat detections that are based on the local definition are specified with a specific name. For example, if a Trojan horse is detected, the scan results

of the Computer Scan displays the threat as Trojan.Foo. You can click the **Run Scans** option available in the **Tasks** window to access the different types of computer scans.

If you suspect that your computer is infected, you can run three types of computer scans manually to prevent virus infections on your computer.

You can run the following types of computer scans:

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. **Quick Scan** takes less time to scan than a Full System Scan because this scan does not scan your entire computer.
Full System Scan	Scans your computer for all types of viruses and security threats. **Full System Scan** thoroughly examines your entire computer for viruses, spyware, and different security vulnerabilities. It also runs LiveUpdate, Virus and Spyware Scan , disk optimization, and backup. In addition, it cleans up the Internet Explorer temporary files and Windows temporary files. Norton 360 automatically runs a Full System Scan when your computer is in idle state.
Custom Scan	Scans a specific file, folder, drive, or removable drive that you choose.

Custom Task	Runs LiveUpdate, backup, and disk optimization tasks. Runs LiveUpdate, backs up your data, frees disk space, and optimizes your disk volume.

Computer Scan provides details about the scanned items. You can view the details such as total number of files scanned, security risks detected, security risks resolved, and the total items that require attention. It also provides you the different ways to resolve any items that were not automatically resolved during the scan. You can also view the severity of the risk, the name of the risk, and the status of the risk about the resolved items.

Running a Quick Scan

A Quick Scan helps you to scan the possible virus-infected areas of a computer that the viruses and other security risks often targets. Because this scan does not scan your entire computer, it takes less time to run than a Full System Scan.

When Norton 360 performs Quick Scan for the first time, it automatically runs LiveUpdate, and cleans up the Internet Explorer temporary files and Windows temporary files.

When the **Insight Protection** option is turned on, Norton 360 simultaneously performs a traditional Quick Scan and an Insight Network Quick Scan. By default, the **Insight Protection** option is turned on.

During idle time, Norton 360 runs a Quick Scan when there is a definition update.

To run a Quick Scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scan**, click **Quick Scan**.

3 Click **Go**.
You can use the following options:

Pause	Suspends the scan temporarily. Click **Resume** to continue the scan.
Skip	Skips the current scan.
Cancel	Terminates a Quick Scan.

4 On the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If there are items require attention, review the risks in the **Threats Detected** window.

Running a Full System Scan

A Full System Scan thoroughly examines your entire computer for viruses, spyware, and different security vulnerabilities. A Full System Scan runs LiveUpdate, virus and spyware scan, disk optimization, and backup.

A Full System Scan helps you to do the following:

- Obtain latest protection and program updates.
- Scan your computer for threats.
- Optimize disks to improve the performance of your computer.
- Back up your data.
  You can back up your files regularly to protect the valuable information on your computer.

To run a Full System Scan

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2 In the **Scans** window, under **Computer Scan**, click **Full System Scan**.

3 Click **Go**.

4 After the scan is complete, in the **Scans** window, click **Close**.

Scanning selected drives, folders, or files

Occasionally, you might want to scan a particular file, removable drives, any of your computer's drives, or any folders or files on your computer. For example, when you work with removable media and suspect a virus, you can scan that particular disk. Also, if you have received a compressed file in an email message and you suspect a virus, you can scan that individual element.

To scan individual elements

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.

2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, do one of the following:

- To scan specific drives, click **Run** next to **Drive Scan**, select the drives that you want to scan, and then click **Scan**.
- To scan specific folders, click **Run** next to **Folder Scan**, select the folders that you want to scan, and then click **Scan**.
- To scan specific files, click **Run** next to **File Scan**, select the files that you want to scan, and then click **Add**.

  You can also press **Ctrl**, and select multiple files to scan.

  You can use the following options to suspend a scan:

Pause	Suspends a custom scan temporarily. Click **Resume** to continue the scan.
Stop	Terminates the scan. Click **Yes** to confirm.

5 In the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If any items require attention, review them on the **Threats Detected** window.

About the Results Summary window

Norton 360 displays the **Result Summary** window when you run a manual scan. At the end of a scan, the **Results Summary** window provides the summary of the scan results.

If your most recent scan was a Quick Scan, this window shows the results of a fast scan of the areas of your

computer. Viruses, spyware, and other risks often target these areas.

If your most recent scan was a Full System Scan, this window shows the results of a comprehensive scan of your entire computer.

The **Result Summary** window displays the following information:

- Total items scanned
- Total security risks detected
- Total security risks resolved
- Total items that require your attention

About the Threats Detected window

Norton 360 displays the **Threats Detected** window when it detects threats. At the end of a scan, the **Threats Detected** window provides you different ways to resolve any items that were not automatically resolved during the scan.

The **Threats Detected** window provides the information such as the severity of the risk, the name of the risk, and the status of the risk. It also provides the action that you can take to resolve the item. The **Threats Detected** window provides you the different options such as **Fix**, **Manual Fix**, **Exclude**, **Get Help**, and **Rescan** to resolve the item.

It also provides the **Ignore** option only once during the first-time detection of low-risk items.

Ignore option is available once until you do not change the default settings for the **Low Risks** option under **Computer Scan**.

The options in the **Threats Detected** window vary based on the types of files that Norton 360 identified as infected during the scan.

About custom scans

You can create a custom scan if you regularly scan a particular segment of your computer. This custom scan lets you scan the segment frequently without having to specify it every time. You can also schedule the custom scan to run automatically on specific dates and times or at periodic intervals. You can schedule a scan according to your preferences. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work.

You can delete the scan when it is no longer necessary. For example, if you work on a project for which you need to swap files frequently with others. In this case, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

Creating a custom scan

Instead of running the default scans that are listed in the **Scans** pane, you can create your own scans that meet your specific requirements. For example, you can create a scan that checks a folder in which you store all the downloaded files.

You can create a custom scan in the **Scans** window.

When you create custom scans, you can also schedule them to run automatically on specific dates and times or at periodic intervals.

To create a custom scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scans**, click **Custom Scan**.
3. Click **Go**.
4. In the **Scans** window, click **Create Scan**.

5 In the **New Scan** window, in the **Scan Name** box, type a name for the scan.
You cannot specify a scan name that is already in use.

6 On the **Scan Items** tab, add the items that you want to scan. See "Selecting the scan items" on page 160.

7 On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 164.

8 On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 161.

9 Click **OK**.

Selecting the scan items

When you configure a custom scan, you must select the items that you want to include in the scan. You can include individual files, folders, or drives. You can include multiple drives, folders, and files to add to the scan. You can also exclude items from the scan.

When you select a drive, all the items in the drive including the files and folders are automatically added to the scan. When you select a folder, all of the files in folder are added to the scan.

To select the scan items

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.

2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, do one of the following:

- To add items for a new scan, click **Create Scan**.
  You must provide a name for the scan in the **Scan Name** box.
- To add items for an existing scan, in the **Edit Scan** column, click the edit icon for the scan that you want to modify.

5 In the window that appears, on the **Scan Items** tab, do the following:

- To add drives, click **Add Drives**, in the **Scan Drives** dialog box, select the drives to be scanned, and click **Add**.
- To add folders, click **Add Folders**, in the **Scan Folders** dialog box, select the folders to be scanned, and click **Add**.
- To add files, click **Add Files**, in the **Files to Scan** dialog box, select the files to be scanned, and then click **Add**.

If you need to remove an item from the list, select the item, and then click **Remove**.

6 Click **OK**.

Configuring the scan options

Norton 360 lets you configure scan options for each scan that you customize. By default, the scan options reflect the current **Computer Scans** settings in the **Settings** window. The changes that you make are applicable to the current scan only.

In addition to the custom scans that you create, you can configure the scan options for the default scans. You can configure scan options for Full System Scan, Quick Scan, Drive Scan, Folder Scan, and File Scan.

To configure the scan options

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.

2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the scan that you want to schedule.

5 In the **Edit Scan** window, on the **Scan Options** tab, configure the scan options as required.

6 Click **OK**.

Editing a custom scan

You can edit a custom scan that you created. You can include additional files or folders to the scan or remove the files and folders that you do not want to scan. You can also change the name of the scan.

You can edit a custom scan in the **Scans** window.

To edit a custom scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scans**, click **Custom Scan**.
3. Click **Go**.
4. In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the custom scan that you want to modify.
5. In the **Edit Scan** window, on the **Scan Items** tab, select the items that you want to scan. See "Selecting the scan items" on page 160.
6. On the **Scan Schedule** tab, set the frequency and time at which you want to perform the scan. See "Scheduling a scan" on page 164.
7. On the **Scan Options** tab, configure the scan options as required. See "Configuring the scan options" on page 161.
8. Click **OK**.

Running a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

You can run a custom scan from the **Scans** window.

To run a custom scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, click **Run** next to the custom scan that you want to run.
You can use the following options to suspend a custom scan:

Pause	Suspends a custom scan temporarily. Click **Resume** to continue the scan.
Stop	Terminates a custom scan. Click **Yes** to confirm.

5 In the **Results Summary** window, do one of the following:

- If no items require attention, click **Finish**.
- If any items require attention, review the risks on the **Threats Detected** window.

Deleting a custom scan

You can delete custom scans if they are no longer needed.

You can delete a custom scan in the **Scans** window.

To delete a custom scan

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.

2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, in the **Delete** column, click the delete icon next to the custom scan that you want to delete.

5 Click **Yes** to confirm that you want to delete the scan.

About scheduling scans

Norton 360 automatically detects the idle state of your computer and runs a Full System Scan. However, you can schedule a Full System Scan according to your preferences. You can also set up a schedule for a Quick Scan and custom virus scans that you create.

You can schedule scans to run automatically on specific dates and times or at periodic intervals. If the scheduled scan begins when you use your computer, you can run the scan in the background instead of stopping your work. Norton 360 lets you schedule the Full System Scan, Quick Scan, and custom virus scans. However, you cannot schedule the Drive Scan, Folder Scan, and File Scan.

You can also set up Norton 360 to turn off your computer or move it to sleep mode or hibernate mode automatically when the scheduled scan is complete.

Scheduling a scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (daily, weekly, or monthly), you are presented with additional options. For example, you can request a monthly scan, and then schedule it to occur on multiple days instead.

In addition to the custom scans that you create, Norton 360 lets you schedule the Full System Scan and Quick Scan.

You can also schedule the scan to run in specific time intervals (hours or days). You can schedule a custom scan in the **Scans** window.

Norton 360 lets you select multiple dates if you schedule a monthly scan.

To schedule a custom scan

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.

2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.

4 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the custom scan that you want to schedule.

5 In the **Edit Scan** window, on the **Scan Schedule** tab, do one of the following:

- If you do not want to run the scan at any particular time, but want to keep the scan options and scan items saved, select **Do not schedule this scan**.
- To run the scan at specific time intervals, select **Run at specific time interval**.
- To run the scan at specific time every day, select **Daily**.
- To run the scan on a specific day on a week, select **Weekly**.
- To run the scan on a specific day on a month, select **Monthly**.

These frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.

6 Under **Run the scan**, do the following:

- To run the scan only at idle time, check **Only at idle time**.
- To run the scan only when your computer is connected with external power source, check **Only on AC power**.
- To prevent your computer from going to a Sleep or Standby mode, check **Prevent standby**.

7 Under **After scan completion:**, select the state at which your computer should be after the scan is complete. Your options are:
   - **Stay On**
   - **Turn Off**
   - **Sleep**
   - **Hibernate**
8 Click **OK**.

Scheduling a Full System Scan

Norton 360 automatically detects the idle state of your computer and runs a Full System Scan. Full System Scan protects your computer against infection without compromising the performance of your computer. You can schedule a Full System Scan on specific dates and times or at periodic intervals.

You can schedule a Full System Scan in the **Scans** window.

To schedule a Full System Scan

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2 In the **Scans** window, under **Computer Scans**, click **Custom Scan**.
3 Click **Go**.
4 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to **Full System Scan**.
5 In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
6 Click **OK**.

Scheduling a Quick Scan

Quick Scan scans the important locations of your computer that the viruses and other security threats often target. When you perform a Quick Scan, Norton 360 scans only the running processes and the loaded programs. Quick Scan takes less time to scan than a Full System Scan because this scan does not scan your entire computer.

Norton 360 lets you schedule a Quick Scan. You can schedule a Quick Scan in the **Scans** window.

To schedule a Quick Scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scans**, click **Custom Scan**.
3. Click **Go**.
4. In the **Scans** window, in the **Edit Scan** column, click the edit icon next to **Quick Scan**.
5. In the **Edit Scan** window, under **When do you want the scan to run?**, set the frequency and time at which you want the scan to run.
   Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
6. Click **OK**.

Editing a scheduled scan

You can change the schedule of any scheduled custom scan, **Quick Scan**, or **Full System Scan** from the **Scans** window.

To edit a scheduled scan from Norton 360 Scans dialog box

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scans**, click **Custom Scan**.

3 Click **Go**.
4 In the **Scans** window, in the **Edit Scan** column, click the edit icon next to the scan that you want to edit.
5 In the **Edit Scan** window, on the **Scan Schedule** tab, change the schedule as required.
Most of the frequency options include the additional options that you can use to refine the schedule. Set the additional options as required.
6 Click **OK**.

About Insight Network scan

The Insight Network scan uses the Cloud technology wherein a remote server on the Web contains the latest virus definitions. Norton 360 scans your computer for the latest security threats. When Norton 360 performs the Insight Network scan, it uses the virus definitions that are available locally and in the Cloud. Norton 360 provides additional protection by using the most recent definitions in the Cloud, apart from the definitions that are available locally on your computer.

Norton 360 performs an Insight Network scan only when the **Insight Protection** option is turned on. By default, the **Insight Protection** option is turned on. You can see this **Insight Protection** option under **Scans and Risks** tab in the **Antivirus** settings window.

When the **Insight Protection** option is turned on, Norton 360 performs a traditional scan and an Insight Network scan simultaneously. The traditional scan uses the definitions from the local system, and the Insight Network scan uses the definitions that are hosted in the Cloud.

Threat detection based on the Cloud definitions is identical to the threat detection that is based on the local definitions. However, the Cloud definitions are specified with additional data about the threats that it detects which indicates that it has been obtained from the Internet. Definitions in the Cloud provide a generic

name for the risk detected, but the local definitions provide the specific name for the risk detected. For example, if a Trojan horse is detected, the scan results of the Insight Network might display Cloud.Trojan. However, the scan results of the local definition might display Trojan.Foo.

If the traditional scan completes while the Insight Network scan is still running, you can view the **Insight Network Scan** progress status.

The Insight Network scan supports Quick Scan, Insight Network context-menu scan, Instant Messenger Scan, and Download Insight scan. It does not support Email Scan, Full System Scan, and Auto-Protect scan.

If the **Insight Protection** option is turned on, you can manually run the following types of Insight Network scans:

- Insight Network Quick Scan

  Norton 360 simultaneously performs a traditional Quick Scan and an Insight Network Quick Scan to scan the areas of your computer that the viruses often target. Norton 360 also performs an Insight Network Quick Scan simultaneously with an Idle Quick Scan.

  The Insight Network scan does not support a Quick Scan that runs as a part of an Idle Full System Scan.

- Insight Network context-menu scan

  When you right-click a file, the shortcut menu displays Norton 360 and then **Insight Network Scan**. You can use this command to scan a file using both local definitions and definitions that are hosted in the Cloud.

  This **Insight Network Scan** command is available only for single file.

Turning off or turning on Insight Protection

Insight Protection option lets Norton 360 perform an Insight Network scan on your computer

When the **Insight Protection** option is turned on, Norton 360 performs a traditional scan and an Insight Network scan simultaneously. The traditional scan uses the definitions from the local system, and the Insight Network scan uses the definitions that are hosted in the Cloud. Norton 360 performs only a traditional scan if the **Insight Protection** option is turned off.

Norton 360 performs an Insight Network scan only when the **Insight Protection** option is turned on. By default, the **Insight Protection** option is turned on.

The Insight Network scan supports only Insight Network Quick Scan, and Insight Network context-menu scan. Insight Network scan does not support a Quick Scan that runs as a part of an Idle Full System Scan. It also does not support Full System Scan, Email Scan, single file Office document scan, and Auto-Protect scan.

To turn off or turn on the Insight Protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click the **Scans and Risks** tab.
4. In the **Insight Protection** row, do one of the following:
   - To turn off Insight Protection, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Insight Protection, move the **On/Off** switch to the left to the **On** position.
5. In the **Settings** window, click **Apply**.

About Reputation Scan

Reputation Scan provides information on the trust-worthiness of all programs and running processes on your computer. It helps you detect the files that are

suspicious or vulnerable on your computer using the reputation-based threat detection. Norton 360 lets you run different types of Reputation Scan and detect suspicious programs on your computer.

Reputation Scan filters the files on the basis of certain filtering criteria and performs an **Insight Network Scan** on the filtered files. Reputation Scan filters the files as reputation files. It filters .exe files, .scr files, .sys files, .dll files, .drv files, .ocx files, .loc files, and .msi files and analyzes these files.

When you perform a Reputation Quick Scan or Full System Scan, Norton 360 considers the Files of Interest that are available on your computer.

After it has filtered the reputation files, Norton 360 performs an **Insight Network Scan**. When Norton 360 performs an **Insight Network Scan**, it also performs a **Computer Scan**. Norton 360 uses the **Computer Scan** to perform the signature-based threat detection. It compares the signature of the filtered reputation files against the known threat signatures to identify threats on your computer. If a security threat is detected, Norton 360 automatically removes the threat from your computer.

Norton 360 uses the **Insight Network Scan** to detect suspicious or vulnerable files on your computer using the reputation-based threat detection. The **Insight Network Scan** uses the Cloud technology wherein a remote Symantec server on the Web stores the latest reputation information. It checks the Cloud for the reputation information on the filtered files.

Norton 360 obtains specific information such as file name and hash key about the filtered reputation files and sends this information to the Cloud. The Cloud analyzes the file information and provides a trust level for each file. The Symantec server sends back the reputation information to your computer. If any of the filtered files is suspicious or vulnerable, Norton 360 assigns **Bad** or **Poor** trust level. Apart from reputation

information, Norton 360 also checks for the latest virus definitions on the Cloud.

Your computer must be connected to the Internet to access the latest reputation information and virus definitions from the Cloud. If your computer is not connected to the Internet, Norton 360 uses the reputation information that is available locally.

When you perform a Reputation Scan, Norton 360 considers only the following categories of files:

Executable files	This category includes Windows executable files (.exe) and script files (.scr).
System files	This category includes Windows System files (.sys), dynamic link library files (.dll), and device driver files (.drv).
Developer files	This category includes ActiveX control files (.ocx).
Miscellaneous files	This category includes Windows Installer Package files (.msi) and resource-only DLL files (.loc).

Norton 360 lets you scan specific areas of your computer based on the type of Reputation Scan that

you select. You can manually run the following types of Reputation Scan:

Quick Scan	Scans the important locations of your computer that the viruses and other security threats often target. When you perform a Quick Scan, Norton 360 considers the Files of Interest that related to loaded programs and the running processes.
Full System Scan	Scans all the Files of Interest that are available on your computer. When you perform a Full System Scan, Norton 360 searches for Files of Interest on all the locations on your computer. The locations include all drives, running processes, loaded programs, and startup files.
Custom Scan	Scans a specific file, folder, drive, or removable drive. When you perform a custom scan, Norton 360 considers only the filtered reputation files.

Symantec rates a file based on the statistical evaluation that is done on the file using the Norton Community

Watch data and Symantec's analysis. Symantec assigns the following confidence levels to reputation files:

Trusted	Symantec has a high indication that the file is trusted.
Good	Symantec has a high indication that the file is trusted.
Unproven	Symantec does not have enough information about the file to assign a trust level to the file. The file is neither safe nor unsafe.
Poor	Symantec has a few indications that the file is not trusted. This file is suspicious and can harm your computer.
Bad	Symantec has a high indication that the file is not trusted. This file is suspicious and can harm your computer.

When the Reputation Scan is complete, you can view the summary of the scan results in the **Norton Reputation Scan** window. You can view the reputation information such as the file name, trust level, age of the file, stability rating, and community usage for each file. The trust level determines whether a file is safe or unsafe. If a file has **Poor** or **Bad** trust level, Norton 360 lets you quarantine the file.

Running a Reputation Full System Scan

When you perform a **Full System Scan**, Norton 360 scans all the Files of Interest that are available on your computer. This fileset includes the files that relate to the running processes, startup files, and loaded programs.

To run a Reputation Full System Scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Reputation Scan**, click **Full System Scan**.
3. Click **Go**.
   In the **Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.
4. If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
5. In the **Quarantine File** window, click **Quarantine this file**.
6. In the **Manual Quarantine** window, click **Add**.
7. Click **Close**.
8. In the **Norton Reputation Scan** window, click **Close**.

Running a Reputation Quick Scan

When you perform a **Quick Scan**, Norton 360 scans only the running processes and the loaded programs. Reputation Quick Scan does not scan your entire computer and it takes lesser time to run than a Reputation Full System Scan.

To run a Reputation Quick Scan

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Reputation Scan**, click **Quick Scan**.

3 Click **Go**.
In the **Norton Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.
4 If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
5 In the **Quarantine File** window, click **Quarantine this file**.
6 In the **Manual Quarantine** window, click **Add**.
7 Click **Close**.
8 In the **Norton Reputation Scan** window, click **Close**.

Running a Reputation custom scan

Norton 360 lets you scan specific areas on your computer by using the Reputation custom scan. You can scan any of your computer's drives, removable drives, folders or files. For example, if you want to check the trust level of a specific file, you can scan the particular file.

To run a Reputation custom scan

1 In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2 In the **Scans** window, under **Reputation Scan**, click **Custom Scan**.
3 Click **Go**.
4 In the **Reputation Custom Scan** window, do one of the following:
- Click **Drive Scan**, select the drive that you want to scan, and then click **Scan**.
- Click **Folder Scan**, select the folder that you want to scan, and then click **OK**.
- Click **File Scan**, select the file that you want to scan, and then click **Open**.

In the **Reputation Scan** window, you can analyze the trust level, prevalence, resource usage, and stability of the scanned items.

5 If there is a file with **Poor** or **Bad** trust level, under the **Trust Level** column, click the red cross (x) icon.
6 In the **Quarantine File** window, click **Quarantine this file**.
7 In the **Manual Quarantine** window, click **Add**.
8 Click **Close**.
9 In the **Norton Reputation Scan** window, click **Close**.

About the Reputation Scan results

Norton 360 lets you run different Reputation Scans to detect any suspicious programs or vulnerable programs on your computer. Norton 360 lets you manually run the following types of Reputation Scan:

- Reputation Quick Scan
- Reputation Full System Scan
- Reputation custom scan

When you run a Reputation Quick Scan, Norton 360 considers the Files of Interest which include running processes and loaded programs. When you run a Reputation Full System Scan, Norton 360 considers all the Files of Interest that are available on your computer. When you run a Reputation custom scan, Norton 360 lets you select the drive, folder, or file that you want to scan.

Reputation Scan filters the files on the basis of certain filtering criteria and performs an **Insight Network Scan** on the filtered files. Reputation Scan filters .exe files, .scr files, .sys files, .dll files, .drv files, .ocx files, and .msi files and analyzes these files.

Norton 360 displays the reputation information of the scanned files in the **Norton Reputation Scan** window.

Norton 360 consolidates the reputation information of your most recent scan and presents the reputation information using different graphical formats.

The top of the **Norton Reputation Scan** window displays the following statistics:

- The **Trust Level** graph displays the average trust level of files on your computer. It also displays the average trust level of the files that Symantec analyzes within the Norton Community.
- The **Prevalence** graph displays the average high user prevalence of files on your computer. It also displays the average high user prevalence of the files that Symantec analyzes within the Norton Community.
- The **Stability** graph displays the average reliable files on your computer. It also displays the average reliable files that Symantec analyzes within the Norton Community.

Stability ratings vary depending upon your operating system.

- The **Norton Network** graph displays the details about the known good files and bad files.

  You can view the number of trusted files that are on your computer. You can also view the total number of files that Symantec analyzes within the Norton Community.

Your computer must be connected to the Internet to view these details. Norton 360 connects to the Symantec servers to collect the reputation information.

The bottom of the **Norton Reputation Scan** window displays the reputation information of each scanned item. For each scanned item, you can view the following details:

File Name	Indicates the file name and file type. You can click a file name to view additional details about the file in the **File Insight** window.

Trust Level

Indicates the trust level that is assigned to a file.

Symantec analyzes specific information about a file such as the digital signature and the hash value to determine the trust level of a file. Symantec rates a file based on the statistical evaluation that is done on the file using the Norton Community Watch data and Symantec's analysis.

Symantec assigns the following trust levels to reputation files:

- **Trusted**: Symantec has a high indication that the file is trusted.
- **Good**: Symantec has a high indication that the file is trusted.
- **Unproven**: Symantec does not have enough information about the file to assign a trust level to the file.
- **Poor**: Symantec has a few indications that the file is not trusted.
- **Bad**: Symantec has a high indication that the file is not trusted.

If you have a file that has **Poor** or **Bad** trust level, Norton 360 displays a red cross (x) icon next to the trust level. You can click on the red cross (x) icon and quarantine the suspicious file.

Prevalence	Indicates the community usage level of the file. The search results are grouped in to the following categories: ■ **Very Few Users**: Shows the files that have very low user prevalence. ■ **Few Users**: Shows the files that have average user prevalence. ■ **Many Users**: Shows the files that have very high user prevalence. You can also use the community usage of a file to determine the legitimacy of the file. Symantec uses a stringent statistical method to evaluate the trustworthiness of a file and to classify the file as a Good file.

Resource Usage	Indicates the system resource usage level of the file. The usage levels are as follows: ■ **Low**: Indicates that the file consumes minimum system resources. ■ **Moderate**: Indicates that the file consumes moderate system resources. ■ **High**: Indicates that the file consumes maximum system resources. ■ **Unknown**: Indicates that the file has performed no action in your computer.

Stability	Indicates the stability rating of the file. The stability rating depends on how frequently the program crashes. The different stability ratings are as follows: ■ **Reliable**: Indicates that the program is reliable. ■ **Stable**: Indicates that the program is comparatively stable. However, it crashes sometimes. ■ **Slightly Unstable**: Indicates that the program is slightly unstable. ■ **Unstable**: Indicates that the program is unstable. ■ **Very Unstable**: Indicates that the program frequently crashes. ■ **Unknown**: Indicates that the crash history of the program is not known. Stability ratings vary depending upon your operating system.

About Scan Facebook Wall

Norton Safe Web protects your computer while you use Facebook. It scans each URL that is available on your Facebook Wall and displays the Norton rating icons for the scanned URLs.

You can also check if a URL is safe or unsafe and then share the URL with your friends on Facebook. Norton Safe Web scans the URL that you post on Facebook and

gives you the safety status for the URL. This way, you are not only protected from unsafe sites but you also let other Facebook users know the security status of any Web site.

However, Norton Safe Web requires your permission to scan the URLs that are available on your Facebook Wall. When you log in to Facebook, Norton Safe Web asks for your permission to access your Facebook Wall. You can choose to allow or deny permission to let Norton Safe Web access your Facebook Wall.

The auto-scan feature in Norton Safe Web application page helps you protect your Facebook Wall. Norton Safe Web scans the News Feed on your Facebook Wall periodically and protects you from malicious links. When Norton Safe Web detects a malicious link, it notifies you with a post on your Facebook Wall. To activate Norton Auto-Scan, go to your **Norton Safe Web** page on Facebook and click **Enable Auto-Scan**.

To remove the malicious link from your Facebook Wall, go to your profile and remove the malicious link. If your friend has posted the malicious link, you can use the **WARN YOUR FRIENDS** option in the message to alert your Facebook friend. You can also click **See Norton Safe Web Report** to view Norton ratings and other details about this malicious link. When no malicious activity is detected on your Facebook Wall, Norton Safe Web posts a message notifying that your Facebook Wall is safe. Norton Safe Web posts this message on your Facebook Wall once in every 30 days.

If you later decide to remove Norton Safe Web from your Facebook profile, you can use the **Application Settings** option of Facebook.

The following are the safety states that Norton Safe Web provides after it scans the links on your Facebook Wall:

Safe	Indicates that the site is safe to visit and Norton Trusted. The sites with this rating do not harm your computer and so you can visit this site.
Warning	Indicates that the site has security risks. The sites with this rating may install malicious software on your computer. Symantec recommends that you do not visit this site.
Untested	Indicates that Norton Safe Web has not yet tested this site and it does not have sufficient information about this site.
Caution	Indicates that the site may have security threats. Symantec recommends you to be cautious while you visit such Web sites.

Scanning your Facebook Wall

The Norton Safe Web feature scans your Facebook Wall and analyzes the security levels of all the available links on your Facebook Wall. It then displays the security status of the scanned URLs. However, Norton Safe Web requires your permission to scan your Facebook Wall.

To scan your Facebook Wall

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Scan Facebook Wall**, click **Scan Facebook Wall**.
3. Click **Go**.
4. In the Facebook login Web page, log in to your Facebook profile.
5. In the **Request for permission** page, click **Allow**.
6. In the Web page that appears, click **Please grant us permission to access your News Feed and Wall**.
7. Follow the on-screen instructions to let Norton Safe Web access your Facebook Wall.

About SONAR Protection

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. SONAR identifies threats quicker than the traditional signature-based threat detection techniques. SONAR detects and protects you against malicious code even before virus definitions are available through LiveUpdate.

SONAR monitors your computer for malicious activities through heuristic detections.

SONAR automatically blocks and removes high-certainty threats. Norton 360 notifies you when high-certainty threats are detected and removed. SONAR provides you the greatest control when low-certainty threats are detected. You can also suppress the SONAR notifications by disabling the **Show SONAR Block Notifications** option.

The **View Details** link in the notification alert lets you view the summary of the resolved high-certainty threats. You can also view the details under **Resolved**

Security Risks category in the **Security History** window.

Turning off or turning on SONAR Protection

SONAR protects you against malicious code even before virus definitions are available through LiveUpdate. By default, SONAR Protection is turned on to proactively detect unknown security risks on your computer.

When you turn off SONAR Protection, you are prompted with a protection alert. This protection alert lets you specify the amount of time for which you want SONAR Protection to be turned off.

When Auto-Protect is turned off, SONAR Protection is also disabled. In this case, your computer is not protected against emerging threats.

To turn off or turn on SONAR Protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. On the **Automatic Protection** tab, under **Real Time Protection**, in the **SONAR Protection** row, do one of the following:
   - To turn off SONAR Protection, move the **On/Off** switch to the right to the Off position.
   - To turn on SONAR Protection, move the **On/Off** switch to the left to the On position.
4. In the **Settings** window, click **Apply**.

About Real Time Exclusions

Symantec Online Network for Advanced Response (SONAR) provides real-time protection against threats and proactively detects unknown security risks on your computer. SONAR identifies emerging threats based on the behavior of applications. SONAR identifies threats quickly compared to the traditional signature-based threat detection techniques. SONAR

detects and protects you from malicious programs even before virus definitions are available through LiveUpdate.

SONAR monitors your computer for malicious activities using heuristic detections. It automatically blocks and removes high-certainty threats. Norton 360 notifies you when high-certainty threats are detected and removed.

However, you can configure Norton 360 to exclude certain programs from the Norton 360 Auto-Protect scans and SONAR scans. You should exclude programs only if you are confident that they are not infected. You can exclude the programs from the Auto-Protect scans and SONAR scans by adding them to the **Real Time Exclusions** window. When you add a program to the **Real Time Exclusions** window, Norton 360 ignores the file when it performs Auto-Protect scan and SONAR scan. This option also excludes subfolders within a folder.

Exclude a program from Norton 360 scans only if you are confident that the program is safe. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer.

To add programs to the **Real Time Exclusions** window, go to the Norton 360 main window, and then click **Settings > Antivirus > Scans and Risks > Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection > Configure**.

Excluding security threats from scanning

You can use **Scan Exclusions** window and **Real Time Exclusions** window to exclude viruses and other high-risk security threats from scanning.

To exclude high-risk security threats from scanning

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.

3 In the **Antivirus** settings window, click the **Scans and Risks** tab.
4 Under **Exclusions / Low Risks**, do one of the following:
   - In the **Items to Exclude from Scans** row, click **Configure**.
   - In the **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection** row, click **Configure**.
5 In the window that appears, click **Add**.
6 In the **Add Item** dialog box, click the browse icon.
7 In the dialog box that appears, select the item that you want to exclude from the scan.
8 Click **OK**.
9 In the **Add Item** dialog box, click **OK**.
10 In the window that appears, click **Apply**, and then click **OK**.

About Signature Exclusions

Norton 360 lets you select specific known security risks and exclude them from Norton 360 scans. Exclude a risk from Norton 360 scans only if you have a specific need. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer. You might also decide not to be notified about the program in future scans.

When you exclude a known security risk from Norton 360 scans, the protection level of your computer reduces. You should exclude items only if you are confident that they are not infected.

To exclude a security risk from scans, you need to add the specific security risk to the **Signature Exclusions** window. The **Signature Exclusions** window contains the list of all security risks that can be excluded from Norton 360 scans. For each security risk, you can view

the risk details and the effect of the risk on your computer.

To add security risks to the **Signature Exclusions** window, go to the Norton 360 main window, and then click **Settings > Antivirus > Scans and Risks > Exclusions / Low Risks > Signatures to Exclude from All Detections > Configure**.

Adding items to the Signature Exclusions

To exclude a security risk from scans, you must add the specific security risk to the **Signature Exclusions** window. You can select a known risk by name and add it to the list.

When you exclude a known security risk from Norton 360 scans, the protection level of your computer reduces. You should exclude items only if you are confident that they are not infected.

To add a signature to the Signature Exclusions

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click the **Scans and Risks** tab.
4. Under **Exclusions / Low Risks**, in the **Signatures to Exclude from All Detections** row, click **Configure**.
5. In the **Signature Exclusions** window, click **Add**.
6. In the **Security Risks** window, click on a security risk that you want to exclude and then click **Add**.
7. In the **Signature Exclusions** window, click **Apply**, and then click **OK**.
8. In the **Settings** window, click **Close**.

About scanning Office documents

Norton 360 protects all Office documents that you receive through email messages, through Internet

download, and through inserted floppy disks or other removable media. By automatically scanning all Office files, Norton 360 maintains a higher level of security. Norton 360 scans the Office document when you open them.

You can use the **Microsoft Office Automatic Scan** option in the **Settings** window to scan documents of the following Microsoft Office applications:

winword.exe	Microsoft Word
excel.exe	Microsoft Excel
powerpnt.exe	Microsoft PowerPoint
visio.exe	Microsoft Visio
msaccess.exe	Microsoft Access
winproj.exe	Microsoft Project

Norton 360 scans the Office documents and protect against threats, including virus macros and infected embedded objects.

By default, **Microsoft Office Automatic Scan** option, under **Computer Scans**, in the **Antivirus** settings window is turned off. Turn on this option to scan Microsoft Office files automatically.

Turning on or turning off Microsoft Office Automatic Scan

Norton 360 maintains a higher level of security by automatically scanning all Office files. You can turn on the **Microsoft Office Automatic Scan** option to protect your computer against the virus macros and embedded objects.

To Turn on or turn off Microsoft Office Automatic Scan

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Antivirus** settings window, click the **Scans and Risks** tab.
4. In the **Microsoft Office Automatic Scan** row, do one of the following:
   - To turn on Microsoft Office Automatic Scan, move the **On/Off** switch to the left to the **On** position.
   - To turn off Microsoft Office Automatic Scan, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, click **Apply**, and then click **Close**.

About Silent Mode

Norton 360 provides many solutions and features to handle viruses and other security threats. Norton 360 displays alerts and notifications to inform you how viruses and other security threats are detected and resolved. When you perform important tasks on your computer, you likely prefer not to receive any alert messages. Norton 360 suppresses alerts and notifications and temporarily suspends most of the background activities based on the **Silent Mode Settings** that are turned on.

Norton 360 provides the following options under Silent Mode Settings:

Silent Mode	Norton 360 allows you to manually turn on for a specified duration using Silent Mode option.

Full Screen Detection	Norton 360 turns on this option automatically when it detects a full-screen application and turns off when you stop using the full-screen application.
Quiet Mode	Norton 360 turns on this option automatically when it detects a disk burning task or a Media Center TV recording task. Norton 360 also turns on Quiet Mode automatically when you run a program that you included in the **Quiet Mode Programs** list. Norton 360 turns off Quiet Mode when the disk burning session or TV program recording session is complete. Norton 360 also turns off Quiet Mode when it stops detecting running instances of the programs that you included in the **Quiet Mode Programs** list.

The Norton 360 icon displays the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. The icon changes to a crescent-patterned icon when Silent Mode is turned on. Norton 360 also notifies you after Silent Mode is turned off.

You can view the summary of the Silent Mode sessions under the **Recent History**, **Full History**, and **Silent Mode** categories in the drop-down list of the **Show** option in the **Security History** window.

The summary includes the following information:

- The turn-on or turn-off status of Silent Mode
- Usage of Silent Mode Settings, such as Silent Mode or Quiet Mode
- The type of program that turns on Silent Mode, such as disk burning or TV recording

- The name of a user-specified program that turns on Silent Mode
- The time and date when Silent Mode is turned on or turned off
- The severity displays the risk level of the selected item

About the Silent Mode that you turn on manually

Norton 360 lets you manually turn on Silent Mode for a specified duration. When Silent Mode is turned on, Norton 360 suppresses alerts and suspends background activities for the duration that you specify. You can verify the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. The Norton 360 icon in the notification area changes to a crescent-patterned icon to display the turn-on status of Silent Mode. Turning on Silent Mode manually before you perform your tasks helps you prevent alerts, notifications, or background activities interrupting you for the specified duration.

You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. After the specified duration, Norton 360 turns off Silent Mode. You can also manually turn off Silent Mode at any time. Norton 360 notifies you after Silent Mode is turned off. The activities that are suspended when Silent Mode is turned on, run after Silent Mode is turned off.

Turning on or turning off Silent Mode manually

You can manually turn on Silent Mode for a specified duration before you perform any important task on your computer. You can turn on Silent Mode for a period of one hour, two hours, four hours, six hours, or one day. The Norton 360 icon displays the turn-on status of Silent Mode in the notification area, at the far right of the taskbar. Norton 360 notifies you after Silent Mode is turned off. After Silent Mode is turned off, Norton 360 also displays alerts if it detected any

security activities that occurred during the Silent Mode session.

You can turn on or turn off Silent Mode from the **Administrative Settings** window, **Quick Controls** in the **Settings** window, or from the **Norton Tasks** window. You can also turn on or turn off Silent Mode by using the Norton 360 icon in the notification area.

To turn on Silent Mode from the Administrative Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **Silent Mode** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.
6. Click **Close**.

To turn off Silent Mode from the Administrative Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Silent Mode Settings**, in the **Silent Mode** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

To turn on Silent Mode from the Norton Tasks window

1. In the Norton 360 main window, click **Performance**.
2. In the **Performance** window, click **Norton Tasks**.
3. In the **Norton Tasks** window, under **Silent Mode**, move the **On/Off** switch to the left to the **On** position.

4 In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.

5 Click **Close** in the **Norton Tasks** window.

To turn off Silent Mode from the Norton Tasks window

1 In the Norton 360 main window, click **Performance**.

2 In the **Performance** window, click **Norton Tasks**.

3 In the **Norton Tasks** window, under **Silent Mode**, move the **On/Off** switch to the right to the **Off** position.

4 Click **Close** in the **Norton Tasks** window.

To turn on Silent Mode from the notification area

1 In the notification area on the Windows taskbar, right-click the Norton 360 icon, and then click **Turn on Silent Mode**.

2 In the **Turn on Silent Mode** dialog box, in the **Select the duration** drop-down list, select how long you want to turn on Silent Mode, and then click **OK**.

To turn off Silent Mode from the notification area

❖ In the notification area on the Windows taskbar, right-click the Norton 360 icon, and then click **Turn off Silent Mode**.

To turn off or turn on Silent Mode from Quick Controls

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Quick Controls**, do one of the following:

- To turn off Silent Mode, uncheck **Silent Mode**.
- To turn on Silent Mode, check **Silent Mode**, and select the duration for which you want Silent Mode to be turned on from the **Turn on Silent Mode** dialog box, and click **OK**.

About the Silent Mode that turns on automatically

When you watch a movie, play games, or make a presentation, you run the application in the full-screen

mode. Norton 360 detects the application that you run in the full-screen mode and automatically enables Silent Mode. When Silent Mode is enabled, Norton 360 suppresses most of the alerts and suspends background activities. Only those activities run that are involved in protecting your computer from viruses and other security threats. Minimum background activities also ensure high performance of your computer. The activities that are suspended run after you finish using the application in the full-screen mode.

Silent Mode also helps you maintain an uninterrupted Media Center Extender session. A Media Center Extender session is an extended session of Media Center to an entertainment device, such as a television. The alerts and notifications that appear during a Media Center Extender session disconnect the session between the host computer and the entertainment device. Norton 360 identifies a Media Center Extender session as an active full-screen application and turns on Silent Mode. When Silent Mode is enabled, Norton 360 suppresses alerts and notifications and suspends background activities to provide uninterrupted sessions for Silent Mode options such as Full Screen Detection or Media Center applications.

Turning off or turning on Full Screen Detection

You can use the **Full Screen Detection** option in the **Settings** window to turn on or turn off Silent Mode automatically when Norton 360 detects a full-screen application. By default, the **Full Screen Detection** option remains turned on after you install Norton 360.

To turn off Full Screen Detection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Full Screen Detection** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.

5 Click **Close**.

To turn on Full Screen Detection

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3 In the **Full Screen Detection** row, move the **On/Off** switch to the left to the **On** position.
4 In the **Settings** window, click **Apply**.
5 Click **Close**.

About Quiet Mode

Norton 360 automatically enables Quiet Mode when you perform tasks that require higher utilization of your system resources. When Quiet Mode is turned on, Norton 360 suspends the background activities and lets the task use the maximum resources for better performance.

You can choose to set Norton 360 to automatically enable Quiet Mode when you do the following tasks:

- IMAPI 2.0 Disk Burn
- Media Center TV Recording
- User-Specified Programs

The following table explains about the various options:

IMAPI 2.0 Disk Burn	When you use a Media Center application to burn a CD or a DVD, Norton 360 automatically enables Quiet Mode, if the **IMAPI 2.0 Disk Burn** option is turned on. By default, the **IMAPI 2.0 Disk Burn** option is turned on. When Quiet Mode is enabled, Norton 360 suspends background activities to improve the performance of your disk-burning session. However, Norton 360 continues to display alerts and notifications during the session. Norton 360 supports the following Media Center disk-burner applications to turn on Quiet Mode: ▪ IMAPI 2.0 ▪ J. River MEDIA CENTER (version 13.0.125 and later) Norton 360 turns on Quiet Mode as soon as you start burning a CD or a DVD using a Media Center application. Norton 360 turns off Quiet Mode after the disk-burning session is complete. You cannot turn off Quiet Mode during the disk-burning session by turning off the **IMAPI 2.0 Disk Burn** option in the **Settings** window.

Media Center TV Recording	When you use a Media Center application to record a TV program, Norton 360 automatically enables Quiet Mode, if the **Media Center TV Recording** option is turned on. By default, the **Media Center TV Recording** option is turned on. When Quiet Mode is enabled, Norton 360 suspends background activities to improve the performance of your TV program recording session. However, Norton 360 continues to display alerts and notifications during the session. Norton 360 supports the following Media Center applications to turn on Quiet Mode: ▪ Windows Media Center For Windows Media Center to enable Quiet Mode during TV program session, you might need to restart your computer after you install Norton 360. ▪ J. River MEDIA CENTER (version 13.0.125 and later) Norton 360 turns on Quiet Mode as soon as you start recording a TV program. After Quiet Mode is turned on, it turns off after the recording session is complete. You cannot turn off Quiet Mode during the TV program recording session by turning off the **Media Center TV Recording** option in the **Settings** window.

User-Specified Programs	Norton 360 automatically turns on Quiet Mode when it detects a TV program recording session or a disk-burning session. In addition, you can manually add the programs for which you want Norton 360 to turn on Quiet Mode to the **Quiet Mode Programs** list. When Norton 360 detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton 360 suspends the background activities but does not suppress alerts and notifications. You can also add or remove a running program to the **Quiet Mode Programs** list.

Turning off or turning on the Quiet Mode options

You can turn off or turn on the Quiet Mode options, such as **IMAPI 2.0 Disk Burn** and **Media Center TV Recording** in the **Settings** window. By default, the Quiet Mode options are turned on. If you perform a task for an option that you turned on, Norton 360 detects the task and automatically turns on Silent Mode. For example, you turn on the **IMAPI 2.0 Disk Burn** option and start burning a disk using a Media Center application. In this case, Norton 360 detects the disk-burning session and turns on Quiet Mode.

Norton 360 turns on Quiet Mode as soon as you start recording a TV program or burning a CD or a DVD. Once Quiet Mode is turned on, it turns off only after the TV program recording session or disk-burning session is complete. You cannot turn off Quiet Mode during the sessions by using the options in the **Settings** window.

To turn off or turn on IMAPI 2.0 Disk Burn

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the Silent Mode Settings, under **Quiet Mode on Detection of**, do one of the following:
   - To turn off detection of a disk burning session, in the **IMAPI 2.0 Disk Burn** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on detection of a disk burning session, in the **IMAPI 2.0 Disk Burn** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

To turn off or turn on Media Center TV Recording

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the Silent Mode Settings, under **Quiet Mode on Detection of**, do one of the following:
   - To turn off detection of a TV program recording session, in the **Media Center TV Recording** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on detection of a TV program recording session, in the **Media Center TV Recording** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

About User-Specified Programs

Norton 360 automatically turns on Quiet Mode when it detects a TV program recording session or a disk-burning session. In addition, you can manually add the programs for which you want Norton 360 to

turn on Quiet Mode to the Quiet Mode Programs list. When Norton 360 detects a running instance of a program that you added in the list, it automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton 360 suspends the background activities but does not suppress alerts and notifications.

You can also add a running program to the Quiet Mode Programs list. However, when you add a running program, Norton 360 does not detect the current running instance of the program to turn on Quiet Mode. Norton 360 turns on Quiet Mode the next time when you execute the program.

You can also remove a running program from the Quiet Mode Programs list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

You can view the details of the programs that you add to the Quiet Mode Programs list or remove from the list in the **Security History** window.

Adding programs to User-Specified Programs

You can manually add the programs for which you want Norton 360 to turn on Quiet Mode to the Quiet Mode Programs list. When you execute the program that you added to the list, Norton 360 detects the program and turns on Quiet Mode.

You can also add a running program to the **Quiet Mode Programs** list. However, when you add a running program, Norton 360 does not detect the current running instance of the program to turn on Quiet Mode. Norton 360 turns on Quiet Mode the next time when you execute the program.

You can only add the programs that have .exe file extension to the **Quiet Mode Programs** list.

To add a program

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the Silent Mode Settings, under **Quiet Mode on Detection of**, in the **User-Specified Programs** row, click **Configure**.
4. In the **Quiet Mode Programs** window, click **Add**.
5. In the **Add Program** dialog box, navigate to the location of the file that you want to add to the Quiet Mode Programs list.
6. Select the file, and then click **Open**.
7. In the **Quiet Mode Programs** window, click **OK**.

Removing programs from User-Specified Programs

You can remove a program from the **Quiet Mode Programs** list. After you remove a program, Norton 360 does not turn on Quiet Mode the next time when it detects a running instance of the program.

You can also remove a running program from the **Quiet Mode Programs** list. However, if Quiet Mode is turned on, it turns off only after the running instances of all the programs in the list are complete. You cannot turn off Quiet Mode by removing a program from the list when it runs.

To remove a program

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Silent Mode Settings** section, under **Quiet Mode on Detection of**, in the **User-Specified Programs** row, click **Configure**.
4. In the **Quiet Mode Programs** window, select the program that you want to delete, and then click **Remove**.

5 In the confirmation dialog box, click **Yes**.
6 In the **Quiet Mode Programs** window, click **Apply** and then click **OK**.

About boot time protection

The boot time protection feature provides enhanced security level from the time you start your computer. It ensures better security by running all the necessary components that are required for computer protection as soon as you start your computer.

To protect your computer during boot time, you must configure the **Boot Time Protection** option. To access the **Boot Time Protection** option, go to the Norton 360 main window, and then click **Settings > Antivirus > Automatic Protection**.

You can use the following options to configure **Boot Time Protection**:

- **Aggressive**

  Provides maximum protection during your computer start time.

  This option ensures complete protection during the boot time as Auto-Protect starts functioning as soon as you start your computer.

- **Normal**

  Provides enhanced protection during your computer start time without compromising your computer's boot performance.

  When you select this option, the drivers and plug-ins start functioning during the computer start time before their specified time delay. This option ensures better boot performance along with good security levels.

- **Off**

  Turns off boot time protection.

  If you turn off the **Boot Time Protection** option, the protection level of your computer reduces.

Configuring boot time protection

The boot time protection feature provides enhanced security level from the time you start your computer. As soon as you start your computer, Norton 360 starts Auto-Protect and all required drivers and plug-ins start functioning. This feature ensures higher level of security from the moment you turn on your computer.

To configure boot time protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Antivirus**.
3. In the **Boot Time Protection** row, click on one of the settings. Your options are:
   - **Aggressive**
   - **Normal**
   - **Off**
4. Click **Apply**, and then click **Close**.

Running a scan at the command prompt

You can scan with Norton 360 from the command prompt without opening the Norton 360 main window. You type the path and name of the file that you want to scan or customize the scan by adding a specific command. The following commands are available:

/?	NAVW32 launches help and terminates.
/A	Scans all drives
/L	Scans the local drives
/S[+|-]	Enables (+) or disables (-) subfolders scanning

/B[+|-]	Enables (+) or disables (-) boot record scanning and master boot record scanning (for example, NAVW32 C: /B+ or NAVW32 C: /B-)
/BOOT	Scans only the boot records
/QUICK	Runs a Quick Scan
/SE[+|-]	Enables (+) or disables (-) a Quick Scan
/ST[+|-]	Enables (+) or disables (-) scanning of stealth items
[folder_path]*[?]	Scans the files that matches specified wild card
[drive|folder|file]	Scans the specified drive, folder, or file
/SESCAN	Performs Quick Scan in the background. Norton 360 displays the **scans** window only when a threat is detected.

To run a scan from the command prompt

1 At the command prompt, type the path in which Norton 360 is located and the executable's file name. The following examples show the syntax of a scan command:

- **`"\Program Files\Norton 360\Engine\version\NAVW32" /command_name`**

  Where *version* represents the version number of Norton 360 and *command_name* represents the command.

- **`"\Program Files\Norton 360\Engine\version\NAVW32" [path]file_name`**

  Where *version* represents the version number of Norton 360 and *[path] file_name* represents the location, name, and extension of the file.

2 Press **Enter**.

Responding to security issues

5

This chapter includes the following topics:

- What to do if a security risk is found

What to do if a security risk is found

Your product provides many solutions and features for handling viruses and other security threats that it detects.

When Norton 360 detects a security risk on your computer, you must take appropriate action on the risk. Norton 360 notifies you when it detects a security risk. You can view details about the risk in the window that appears and select an action that you want Norton 360 to perform on the risk.

By default, Norton 360 removes the security risk from your computer and quarantines it. However, you can restore the file from the Quarantine to its original location and exclude it from future scans.

Exclude a program from Norton 360 scans only if you are confident that the program is safe. For example, if another program relies on a security risk program to function, you might decide to keep the program on your computer.

In some cases, Norton 360 requires your attention to manually resolve the detected security risk. You can access the Symantec Security Response Web site and refer the manual removal instructions.

In some cases, Norton 360 might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can submit the item to Symantec for further analysis.

In addition, your product provides solutions for security risks, such as spyware and adware.

About detecting viruses, spyware, and other risks

Viruses and other security threats can be detected during a manual or customized scan. Auto-Protect detects these threats when you perform an action with an infected file. Threats can also appear during an instant messenger session, when you send an email message, or during a manual or customized scan.

Security risks, such as spyware and adware, can also be detected when these activities are performed.

The files that can potentially infect your system when your computer first starts up are scanned first.

These files include the following:

- Files that are associated with the processes that are currently running in memory
- Files with startup folder entries
- Files with system start INI file entries
- Files with system start batch file entries
- Files that the system start registry keys refers

If an infected file is detected during this portion of the manual scan, it is repaired or removed. Any unnecessary references are also removed from your computer. Before attempting to repair, quarantine, or delete any infected file that has a process running in memory, your product attempts to terminate the process. You are alerted and prompted to close all unnecessary programs before the process is terminated.

You can view information about detected viruses and other security threats in Security History.

Security History also includes information about spyware, adware, and other security risks.

Reviewing Auto-Protect notifications

Auto-Protect scans files for viruses, worms, and Trojan horses when you perform an action with them, such as moving them, copying them, or opening them.

It also scans for spyware, adware, and other security risks.

If Auto-Protect detects suspicious activity, it logs a notification in Security History that tells you that a risk was found and resolved.

If Auto-Protect detect one or more viruses it either repairs or deletes the viruses and notifies you. The notification provides information on which file was repaired or deleted and which virus, Trojan horse, or worm infected the file. No further action is necessary.

To review Auto-Protect notifications

1. In the Norton 360 main window, click **Tasks**.
2. In the **Tasks** window, under **General Tasks**, click **Check Security History**.

3 In the **Show** drop-down list, select the category for which you want to review Auto-Protect alerts. Your options are:

Recent History	Review Auto-Protect notifications that you received in the last seven days.
Full History	Review all of the Auto-Protect notifications that you have received.
Resolved Security Risks	Review all of the resolved security threats. The **Resolved Security Risks** category includes the infected files that Norton 360 repairs, removes, or quarantines.
Unresolved Security Risks	Review the list of unresolved security risks. The **Unresolved Security Risks** category includes the infected files for which Norton 360 was not able to take any action. This category mostly includes the low-level risks that require your attention for a suitable action.

4 In the right pane, click the **Options** link.
The option name appears as **Restore & Options** for few items.
If one or more security risks such as spyware are found, you can take action on these items, if required.

5 In the **Threat Detected** window, select the appropriate action on the risk.
The following are some of the options that are available in the **Threat Detected** window:

Restore & Exclude this file	Returns the selected Quarantine item to its original location and excludes the item from being detected in the future scans. This option is available for the detected viral and non-viral threats.
Exclude this program	Excludes the security risk from future scan. Norton 360 adds the security risk to the appropriate exclusions list.
Manual Fix (recommended)	Lets you resolve the risk using a manual fix tool. If you resolve a threat manually, you must remove the threat information from the **Security History** window.
Remove this file (may cause browser to close) (recommended)	Removes the security risk from your computer and quarantines it. This option is available for the security risks that require your attention.

Remove this file (may cause browser to close)	Removes the selected security risk from the computer and quarantines it. This option is available for the security risks that require your attention for manual removal. This option is also available for the security risks that are manually quarantined.
Remove from history	Removes the selected security risk item from the Security History log.
Get help (recommended)	Takes you to the Symantec Security Response Web site. This option is available for the security risks that require your attention for manual removal. You can refer the Symantec Security Response Web site for manual removal instructions or other information about the risk.

Submit to Symantec	Sends the security risk to Symantec. In some cases, Norton 360 might not identify an item as a security threat, but you might suspect that the item is infected. In such cases, you can use this option to submit the item to Symantec for further analysis.

About responding to risks detected during a scan

At the end of a scan, the **Results Summary** window provides the summary of the scan results. You can use the **Threats Detected** window to resolve any items that were not automatically resolved during the scan.

You can use the **Show** drop-down list that is available in the **Security History** window to resolve any items that were not automatically resolved during the scan. The **Recommended Action** section in the **Security History** window displays the action that you should take to resolve the security threat.

If you have run a Full System Scan, Norton 360 displays the **Scans** window at the end of the scan. The **Scans** window lists each activity and status of the scan results.

About actions when Norton 360 cannot repair a file

One of the common reasons that Norton 360 cannot automatically repair or delete an infected file is that you do not have the current definition updates. Run LiveUpdate, and then scan again.

Before running LiveUpdate to receive protection updates, ensure that Quick Scan is turned on (it is turned on by default). After LiveUpdate retrieves the latest definition updates, Quick Scan automatically

checks for the infections that have processes running in memory. It also checks for the infections that the start-up files and folders refer.

If that does not work, read the information on the **Security History - Advanced Details** window to identify the types of files that cannot be repaired. You can take one of the following actions, depending on the file type:

Infected files	You can view the file type of the detected risk. This information helps you to decide the action that can be taken depending on the file type. For example, you can view the infected files with the following file name extensions (any file can be infected): ▪ .exe ▪ .doc ▪ .dot ▪ .xls
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using your operating system disks.

Understanding alerts and messages

6

This chapter includes the following topics:

- About Norton 360 alerts and messages
- About managing messages and alerts
- Types of risks
- Types of threats
- Types of viruses

About Norton 360 alerts and messages

Most of the time, Norton 360 quietly protects your computer from viruses and other risks and threats so that you can use your PC with confidence. The green badge on the Norton 360 status icon in the lower-right corner of your computer screen indicates that your protection is up to date. You can use your computer with confidence. If the badge color changes to orange or red, it means you should open Norton 360 to learn about the problems that Norton 360 has encountered.

About managing messages and alerts

Norton 360 displays messages in several ways and in several locations.

You might see messages in the following locations:

Notification area on your Windows desktop	Several types of Norton 360 messages appear in the notification area, at the far right of the taskbar. For example, your PC was turned off, or it has not been connected to the Internet for a while. In this case, you see a message that your protection may not be up to date. A different alert appears if a security setting was turned off. This message warns you that your PC might not be secure and helps you to turn on the setting. In most cases you can click the alert to open Norton 360 and fix the problems.
Norton 360 main window overall status	Alerts and other messages appear at the middle of the main window. The color of the message indicates its urgency. If the message color is green, your computer is protected. If the message color is orange or red, you must take appropriate action to ensure that you stay protected.

Norton 360 protection categories and details	Norton 360 displays individual status areas for each protection feature, such as **PC Security**, **Identity**, **Backup**, and **PC Tuneup**. The status areas show how many issues need to be resolved for each feature. You can use **View Details** under each status area for more information about those issues. You can use the **Fix Now** option to fix all the issues that need to be resolved to secure your computer.
Norton 360 gadget in the Windows sidebar	In Windows Vista and Windows 7, Norton 360 displays the security status of your computer in the Norton 360 gadget in the Windows sidebar.

Types of risks

A risk is anything that can be exploited to harm your PC and its data, or that can be used to steal your data. Norton 360 protects your system from a variety of risks.

Risks fall into several categories:

Malicious software	These programs are deliberately designed to cause damage to your PC. They include threats such as viruses, worms, and Trojan horses. Malicious software is sometimes called malware.

Spyware	These programs conceal themselves on your PC. They monitor what you do, or look through the information that is stored on your PC, and send the information back to their creators.
Vulnerabilities	These risks consist of flaws in legitimate software that can be exploited, either to cause damage, block data, or steal information. Vulnerabilities are usually exploited through network connections.

Types of threats

Threats consist of the software that has been deliberately designed to destroy, modify, disclose, or block your data.

Threats fall into the following categories:

Viruses	Viruses are the small programs that attach themselves to other programs and replicate themselves.
Worms	Worms are like viruses in that they copy themselves from PC to PC, but they do not attach themselves to other programs.

Trojan horses	These destructive programs claim to be some other type of program, but they cause damage when they run.

Norton 360 scans your PC for viruses, worms, Trojan horses, and other software that is intentionally destructive. It also monitors your Internet connection to protect you from the Internet-based threats that exploit software vulnerabilities.

Types of viruses

A virus is a small program that is designed to alter the way your PC operates, without your knowledge or permission.

To be a virus, a program must do the following:

- Run on its own, without you having to take any action
- Make copies of itself so that it can spread to other PCs

Although not all viruses are intended to cause damage, even harmless viruses can affect the performance and stability of your PC. Norton 360 attempts to remove all viruses from your PC.

Viruses fall into the following recognized categories:

File infectors	These viruses infect program files. When infected files run, they can attach the viruses that they carry to other program files. Norton 360 scans all program files on your PC to find and eliminate file infectors.

Boot viruses	These viruses attach themselves to the system areas of your PC and become active as soon as your PC starts. They can attach themselves to disks or other storage devices that is connected to your PC. Norton 360 scans the system areas of your PC to find and remove boot viruses.
Multipartite viruses	These viruses use the techniques of both boot and file infector viruses. Norton 360 scans for such viruses and eliminates them.
Macro viruses	These viruses attach themselves to the data files that contain executable components, such as some spreadsheet, presentation, and word-processing files. These viruses that are spread when a program runs the executable portion of a data file. Norton 360 scans data files for macro viruses and removes them.

Norton 360 scans your PC for both known viruses and unknown viruses.

Known viruses are automatically detected and repaired. Unknown viruses are detected by analyzing each executable file for various characteristics common to viruses. In addition, Norton 360 automatically updates itself over the Internet to expand and refine its list of known viruses.

Doing routine tasks

7

This chapter includes the following topics:

- Turning on or turning off automatic tasks
- About custom task
- About scheduling automatic tasks
- About scheduling backups
- Specifying Idle Time Out duration

Turning on or turning off automatic tasks

Norton 360 runs automatic tasks as it quietly works to protect your PC. These automatic tasks include scanning for viruses, monitoring your Internet connection, updating backups, and downloading protection updates. These activities run in the background when your PC is turned on.

If any item needs your attention, Norton 360 displays a message that tells you the current status or asks you to do something. If you do not see any messages, then Norton 360 is doing its job and your PC is protected.

You can open Norton 360 at any time to see the status of your PC at a glance or to view protection details.

When a background activity is in progress, Norton 360 notifies you with a message in the notification area that is located at the far-right of the task bar. You can

see the results of the latest Norton 360 activities the next time you open the Norton 360 main window. To see a current report of Norton 360 activities, you can view the summary in the **Monthly Report** window.

To turn on or turn off automatic tasks

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Tasks Scheduling**.
3. In the **Task Scheduling** window, on the **Automatic Tasks** tab, do the following:
   - Check the feature that you want to run automatically.

     Check the **Tasks** check box to check all the features at once.
   - Uncheck the feature that you do not want to run automatically.

     Uncheck the **Tasks** check box to uncheck all the features at once.
4. Click **Apply**.
5. Click **Close**.

About custom task

Norton 360 lets you choose your own combination of tasks for a one-time scan. You can run LiveUpdate, back up your data, remove temporary files, free disk space by cleaning up disk clutter, and optimize your disks.

You can select and run the following tasks:

LiveUpdate	Downloads the latest protection and program updates.

Internet Explorer Temporary Files	Deletes the temporary files that are left behind on your PC's hard disk after Internet browsing.
Windows Temporary Files	Deletes the unnecessary files that are left in Windows Temporary folders after a program has been installed or updated.
Internet Explorer History	Deletes the unnecessary Web page history that is left behind in your Internet browser's history folder.
Disk Optimization	Defragments your hard disk and free space.
Registry Cleanup	Deletes the inaccurate entries and obsolete entries in the Windows registry that can cause errors.
Backup	Runs backup. The files to be backed up and the backup location are the ones you specified when you configured your backup settings.

Running custom tasks

Norton 360 automatically checks your system and chooses the best settings to keep your system secure. However, you can run some specific tasks. You can choose the specific tasks that you want to run by using the options available in the **Custom Tasks** window.

Norton 360 lets you choose your own combination of tasks for a one-time scan. You can run LiveUpdate, back up your data, free disk space by cleaning up disk clutter, and optimize your disks.

To run custom tasks

1. In the Norton 360 main window, click **PC Security**, and then click **Run Scans**.
2. In the **Scans** window, under **Computer Scan**, click **Custom Task**, and then click **Go**.
3. In the **Custom Tasks** window, check the tasks that you want to run.
   To select all the tasks, check the **Tasks** option.
4. Click **Go**.

About scheduling automatic tasks

You can use the Task Scheduling settings to specify how often Norton 360 scans your system for security and performance issues. You can also access backup scheduling options from Task Scheduling settings.

Scheduling security and performance scans

Use the Task Scheduling settings to have Norton 360 examine your system automatically for security and performance issues. You can specify when and how often Norton 360 performs those examinations.

You have the following options for scheduling security and performance scans:

Automatic (Recommended)	Examine your PC for security and performance issues whenever your PC is idle. This setting provides the maximum protection.

Weekly	Examine your PC one or more times each week for security and performance issues. You can pick the days of the week and the time of day on which the scan performs.
Monthly	Examine your PC once each month for security and performance issues. You can pick the day of the month and the time of day on which the scan performs.
Manual Schedule	Do not perform a scheduled security or performance scan of your PC. If you choose this option, you should perform manual security and performance scans of your PC periodically to maintain protection.

Your computer's performance is maximized if you schedule your critical operations to occur when your computer is idle. When you schedule your scans weekly or monthly and check the **Run only at idle time** option, Norton 360 scans your computer when it is idle. Symantec recommends that you check **Run only at idle time** to experience better performance of your computer.

To schedule security and performance scans

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, click **Tasks Scheduling**.

3 On the **Scheduling** tab, under **Schedule**, select an option.
When you click **Weekly** or **Monthly**, you must select the time and day to run the automatic tasks. You also have the option of specifying that the automatic tasks must run only when the PC is idle.
4 Click **Apply**.
5 Click **Close**.

About scheduling backups

You can configure backup scheduling on the **When** tab in the **Manage Backup Sets** window to specify when and how often should Norton 360 back up your files.

You have the following backup scheduling options:

Automatic (Recommended)	Backs up the changed files whenever your PC is idle This setting provides the best backup protection.
Weekly	Backs up the changed files one or more times each week You can pick the days of the week and the time of day on which Norton 360 should perform backups.
Monthly	Backs up the changed files once each month You can pick the day of the month and the time of day on which Norton 360 should perform backups.

Manual Schedule	Does not perform any scheduled backups of changed files If you choose this option, you should manually back up your changed files regularly.

Your computer's performance is maximized if you schedule your critical operations to occur when your computer is idle. When you schedule backup weekly or monthly and check **Run only at idle time**, Norton 360 backs up your files when your computer is idle. Symantec recommends that you check **Run only at idle time** to experience better performance of your computer.

Specifying Idle Time Out duration

You can set the duration after which Norton 360 should identify your computer as idle. You can select a value (in minutes) between 1 minute and 30 minutes. When you do not use your computer for the specified duration, Norton 360 identifies your computer as idle. Norton 360 then runs the activities that are scheduled to run at idle time.

To specify Idle Time Out duration from the Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the **Idle Time Out** row, in the drop-down list, select the duration that you want to specify. You might need to scroll the window to view the option.
4. In the **Settings** window, click **Apply**.

Keeping secure on the Internet

8

This chapter includes the following topics:

- About the Smart Firewall
- About Intrusion Prevention
- About Download Insight
- About Norton AntiSpam
- About configuring POP3 and SMTP ports
- About Metered Broadband Mode

About the Smart Firewall

The Smart Firewall monitors the communications between your computer and other computers on the Internet. It also protects your computer from such common security problems as the following:

Improper connection attempts	Warns you of connection attempts from other computers and of attempts by programs on your computer to connect to other computers

Port scans	Cloaks the inactive ports on your computer thereby providing protection against attacks through hacking techniques such as port scanning
Intrusions	Monitors the network traffic to or from your computer for suspicious behavior and stops any attack before they threaten your system

A firewall blocks hackers and other unauthorized traffic, while it allows authorized traffic to pass. Turning off Smart Firewall reduces your system protection. Always ensure that the Smart Firewall is turned on.

Turning off or turning on Smart Firewall

Smart Firewall monitors communications between your computer and the other computers on the Internet. It also protects your computer from common security problems.

If you must turn off the Smart Firewall, you should turn it off temporarily to ensure that it is turned on again automatically. To ensure that your computer remains protected, you can turn on the Smart Firewall manually before the time that you specify concludes.

When the Smart Firewall is turned off, your computer is not protected from Internet threats and security risks.

To turn off Smart Firewall

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **General Settings** tab, in the **Smart Firewall** row, move the **On/Off** switch to the right to the **Off** position.
4 Click **Apply**.
5 In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off Smart Firewall.
6 Click **OK**.
7 Click **Close**.

To turn on Smart Firewall

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **General Settings** tab, in the **Smart Firewall** row, move the **On/Off** switch to the left to the **On** position.
4 Click **Apply**.
5 Click **Close**.

To turn off Smart Firewall from Quick Controls

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Quick Controls**, uncheck **Smart Firewall**.

To turn on Smart Firewall from Quick Controls

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Quick Controls**, check **Smart Firewall**.

To turn off Smart Firewall from the notification area

1 In the notification area on the taskbar, right-click the Norton 360 icon, and then click **Disable Smart Firewall**.
2 In the **Security Request** window, in the **Select the duration** drop-down list, select the duration for which you want to turn off Smart Firewall.
3 Click **OK**.

To turn on Smart Firewall from the notification area

- In the notification area on the taskbar, right-click the Norton 360 icon, and then click **Enable Smart Firewall**.

About firewall rules

A firewall is a security system that uses rules to block or allow connections and data transmission between your computer and the Internet. Firewall rules control how the Smart Firewall protects your computer from malicious programs and unauthorized access. The firewall automatically checks all traffic that comes in or out of your computer against these rules.

The Smart Firewall uses two kinds of firewall rules:

Program rules	Control network access for programs on your computer.
Traffic rules	Control all the incoming and the outgoing network traffic.

About the order in which firewall rules are processed

The Smart Firewall processes Traffic rules before it processes Program rules. For example, when there is a Program rule that allows Internet Explorer to access Internet using port 80 with TCP protocol and a Traffic rule that blocks TCP communication through port 80 for all applications. The Internet Explorer application cannot access the Internet as Norton 360 gives precedence to Traffic rules over the Program rules.

For example, you have a Program rule for the Symantec pcAnywhere application that blocks the use of the application with any other computer. You add another rule for the same application that allows its use with a specific computer. You then move the new rule before the original rule in the program rule list. Norton 360 processes the new rule first and lets you use Symantec

pcAnywhere with that specific computer. It then processes the original rule and prevents its use with any other computer.

About Traffic rules

Norton 360 includes a number of predefined Traffic rules. These rules provide network functionality and protection from known Internet risks. Examples of default Traffic rules include the following:

Default Allow Specific Inbound ICMP Default Allow Specific Outbound ICMP	Permit all types of outbound and safe types of inbound ICMP (Internet Control Message Protocol) messaging. ICMP messages provide status and control information.

Default Allow Inbound NetBIOS Name (Shared Networks) Default Allow Inbound NetBIOS (Shared Networks)	Permit the use of the NetBIOS name service and the NetBIOS datagram service that the Microsoft Network uses in file and printer sharing. NetBIOS is an acronym for Network Basic Input/Output System. NetBIOS provides name service, session service, and datagram service. Name service provides resolution of names, Session service manages sessions for connection-oriented services, and Datagram service distributes datagrams for connection-oriented services.
Default Allow Inbound Bootp Default Allow Outbound Bootp	Permit the use of the Bootp service. Bootp is short for Bootstrap Protocol, which enables a computer to discover its own IP address.

The **Traffic Rules** tab displays a list of predefined traffic rules. Some of the default Traffic rules are read-only and are locked. You cannot modify these rules.

The rules appear in the order of their priority levels. Rules that appear higher in the list override the rules that appear lower in the list.

You can add a new Traffic rule on this tab. You can also do the following activities:

Modify a Traffic rule	You can change the settings of a Traffic rule that does not function the way you want. However, you cannot modify some of the default rules that are read-only. See "Modifying Traffic rules and Program rules" on page 254.
Turn off a Traffic rule	You can disable a Traffic rule. However, you cannot turn off some of the default rules that are read-only. See "Turning off a Traffic rule temporarily" on page 256.
Change the priority of a Traffic rule	You can change the priority of a Traffic rule by changing where it appears in the list. Only advanced users or novice users at the direction of technical support, should perform this action. See "Changing the order of firewall rules" on page 255.

About Program rules

Program rules control network access for the programs that are on your computer. You can use the **Firewall** settings to create and modify rules for programs.

On the **Program Rules** tab, you can do the following:

- Add a program.
- Rename a program.

- Modify the rules for a program.
- Add a rule for a program.
- Modify the access settings of a program rule.
- Modify the priority of rules for a program by changing the sequence of rules in the list.
- Remove a program rule.
- Remove a program.

You can create Program rules in the following ways:

Automatically customize Internet access settings	Lets the firewall automatically configure access for programs the first time that users run them. This method is the easiest way to create firewall rules.
Use Firewall settings	Manages the list of programs that can access the Internet.

Respond to alerts	Lets the firewall notify you when a program attempts to access the Internet. You can then allow or block Internet access for the program. In some instances, such as when you watch a movie, you might prefer not to be alerted with any messages. In such cases, you can turn on Automatic Program Control. Norton 360 does not prompt you with any firewall alerts in this state. The firewall notifies you only if you have changed the **General Settings** options of Smart Firewall from their default, recommended settings.

Adding a program to Firewall settings

You can add programs to Firewall settings to control their ability to access the Internet. Manually configured Firewall settings for programs override any settings that Automatic Program Control makes. However, Symantec recommends you to retain the settings that Automatic Program Control makes as and when you run your programs.

Firewall settings for programs are not migrated from previous versions of Norton 360. If you want to restore any programs that you manually added in the previous version, you must add them again in the current version.

To add a program to Firewall settings

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Program Rules** tab, click **Add**.
4. In the **Select a program** dialog box, browse to the executable file for the program that you want to add.
5. Click **Open**.
6. In the **Security Request - Program Control** window, in the **What do you want to do?** drop-down list, select the access level that you want this program to have. Your options are:

Allow	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet access (Recommended)	Create the rules that control how this program accesses the Internet. You can set the following criteria for a rule: ▪ **Action** ▪ **Connections** ▪ **Computers** ▪ **Communications** ▪ **Advanced** ▪ **Description** If you select this option, you must follow the instructions in the wizard that appears and configure the rule.

7 Click **OK**.

Customizing a program

After you use Norton 360 for a while, you might need to change the access settings for certain programs.

To customize a program

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Program Rules** tab, in the **Program** column, select the program that you want to change.
4 In the drop-down list next to the program that you want to change, select the access level that you want this program to have. Your options are:

Allow	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Custom	Create the rules that control how this program accesses the Internet.

The **Auto** option is the default option that is assigned automatically to a program when Automatic Program Control is turned on.

5 Click **Apply**.

Removing a program

You can remove programs from Firewall settings if necessary.

The firewall settings for the programs are not migrated from previous versions of Norton 360. If you removed any programs in the previous version and do not want

them in the current version, you must remove them again.

To remove a program from Firewall settings

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Program Rules** tab, in the **Program** column, select the program that you want to remove.
4. Click **Remove**.
5. In the **Confirmation** dialog box, click **Yes**.
   The confirmation dialog box appears only when the **Automatic Program Control** option is turned off.
6. Click **Apply**.

Adding Traffic rules and Program rules

Firewall settings automatically create most of the firewall rules that you need. You can add custom rules if necessary.

Only experienced users should create their own firewall rules.

You can add the following types of firewall rules:

- Traffic rules
- Program rules

To add a Traffic rule

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Traffic Rules** tab, click **Add**.
4. Follow the instructions in the **Add Rule** wizard.

To add a Program rule

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **Program Rules** tab, in the **Program** column, select the program to which you want to add a rule.
4 Click **Modify**.
You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
5 In the **Rules** window, click **Add**.
6 Follow the instructions in the **Add Rule** wizard.
7 In the **Rules** window, click **OK**.

Using the Add Rule Wizard

The **Add Rule** Wizard leads you through the steps that are necessary to create firewall rules.

To use the Add Rule Wizard

1 Open the **Add Rule Wizard** by creating a Traffic rule or a Program rule.

2 In the first panel of the **Add Rule Wizard**, select the action that you want for this rule. Your options are:

Allow	Allow communication of this type. For example, consider a Traffic rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Allow**, Smart Firewall allows all connections that satisfy the criteria of this Traffic rule.
Block	Prevent communication of this type. For example, consider a Traffic rule with the following criteria: all inbound connections from Internet address 192.168.1.1 through port 8080. When you select **Block**, Smart Firewall blocks all connections that satisfy the criteria of this Traffic rule.

Monitor	

	Update the **Firewall – Activities** category in the event log each time that communication of this type takes place. This option lets you monitor how often this firewall rule is used. Norton 360 notifies you every time that the traffic matching the monitor rule criteria passes through your computer. You can use the links in these notifications to view the logs. You can view the event log under **Firewall – Activities** category in the **Security History** window. Norton 360 creates separate action rules to allow or block the programs that have only a **Monitor** rule associated with them. The **Monitor** rule must be of higher order than the action rule for successful log entry of the network event that is related to the program. The monitor rule only logs the traffic events in the **Security History** window. You need to create another Allow or Block rule to handle the network traffic. You can monitor and allow or block the traffic by enabling the **Create a**

	Security History log entry option in the **Add Rule Wizard** or the **Modify Rule Wizard**.

3 Click **Next**.

4 Select the type of connection for the rule. Your options are:

Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to inbound and to outbound connections.

5 Click **Next**, and then select the computers that apply to the rule. Your options are:

Any computer	The rule applies to all computers.
Any computer in the local subnet	This rule applies only to computers in the local subnet. An organization's network is divided into subnets to facilitate efficient Internet communications. A subnet represents all of the computers in the same LAN.

Only the computers and sites listed below	The rule applies only to the computers, sites, or domains that you specify. You can specify the names and addresses of computers that apply to the rule. The details of the specified computers appear in the list. You can also remove computers from the list. When you select this option, the **Add** option becomes available. When you click **Add**, Norton 360 displays the **Networking** dialog box in which you can specify individual computers, a range of computers, or specify all computers on a subnet or network. You can use the **Add** option or the **Remove** option to add or remove a computer.

6 Click **Next**, and then select the protocols for the rule. Your options are:

TCP	The rule applies to TCP (Transmission Control Protocol) communications.
UDP	The rule applies to UDP (User Datagram Protocol) communications.
TCP and UDP	The rule applies to TCP and to UDP communications.
ICMP	The rule applies to ICMP (Internet Control Message Protocol) communications. This option is available only when you add a Traffic rule, modify a Traffic rule, or modify a Program rule that handles ICMP traffic.
ICMPv6	The rule applies to ICMPv6 (Internet Control Message Protocol for Internet Protocol version 6) communications. This option is available only when you add a Traffic rule, modify a Traffic rule, or modify a Program rule that handles ICMPv6 traffic.

All	The rule applies to all supported protocols. When you select this option, you cannot specify the types of communications or ports that apply to the rule.

7 Select the ports for the rule. Your options are:

All types of communication (all ports, local and remote)	The rule applies to communications that use any port.
Only communications that match all types and ports listed below	The rule applies to the ports that you specify. You can specify the ports by selecting from the listed ports or by adding specific ports or port ranges. If you select ICMP or ICMPv6 protocol, you can specify the commands. To do so, select a command from the list of known commands or add specific commands or command ranges. When you select this option, the **Add** option becomes available. You can use the **Add** option or the **Remove** option to specify or remove a port or a command.

8 Click **Next**.

9 Check **Create a Security History log entry** if you want Norton 360 to create an entry in the firewall event log.
Norton 360 creates an entry when a network communication event matches this rule. You can view the event log in the **Security History** window under **Firewall – Activities**. If you selected the **Monitor** option in the **Action** window, then the **Create a Security History log entry** option is automatically checked. You cannot uncheck the box to turn off this option as it is the default setting.

10 Check **Apply this rule** if you want to apply this rule to IPv6 NAT Traversal traffic.

11 Click **Next**, and then, in the text box, type a name for this rule.

12 Click **Next**, and then review the new rule settings.

13 Click **Finish**.

14 When you have finished adding rules, click **OK**.

Modifying Traffic rules and Program rules

You can change an existing firewall rule if it does not function the way that you want. You can use the **Modify** option to change the settings of an existing firewall rule. When you change a rule, the firewall uses the new criteria of the modified rule to control network traffic.

You cannot modify some of the default rules that are read-only. However, you can view the settings of these rules by using the **View** option.

To modify a Traffic rule

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **Traffic Rules** tab, select the rule that you want to change.

4 Click **Modify**.

5 In the **Modify Rule** window, make the necessary changes to modify any aspect of the rule.
6 When you have finished changing the rule, click **OK**.

To modify a Program rule

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Program Rules** tab, select the program that you want to change.
4 Click **Modify**.
You can also use the **Access** drop-down list next to the program to modify the access level for the program. Accordingly, Smart Firewall modifies or creates the relevant rule for the program.
5 In the **Rules** window, select the rule that you want to change.
6 Click **Modify**.
7 In the **Modify Rule** window, make the necessary changes to modify to change any aspect of the rule.
8 When you have finished changing the rule, click **OK**.
9 In the **Rules** window, click **OK**.

Changing the order of firewall rules

Each list of firewall rules is processed from the top down. You can adjust how the firewall rules are processed by changing their order.

Do not change the order of the default Traffic rules unless you are an advanced user. Changing the order of default Traffic rules can affect firewall functionality and reduce the security of your computer.

To change the order of Traffic rules

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **Traffic Rules** tab, select the rule that you want to move.
4 Do one of the following:
   - To move this rule before the rule above it, click **Move Up**.
   - To move this rule after the rule below it, click **Move Down**.
5 When you are done moving the rules, click **Apply**.

To change the order of Program rules

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Program Rules** tab, select the program that contains the rule that you want to move.
4 Click **Modify**.
5 In the **Rules** window, select the rule that you want to move.
6 Do one of the following:
   - To move this rule before the rule above it, click **Move Up**.
   - To move this rule after the rule below it, click **Move Down**.
7 When you are done moving the rules, click **OK**.
8 In the **Firewall** settings window, click **Apply**.

Turning off a Traffic rule temporarily

You can temporarily turn off a Traffic rule if you want to allow specific access to a computer or a program. You must remember to turn on the rule again when you are done working with the program or computer that required the change.

You cannot turn off some of the default firewall rules that appear in the list. You can only view the settings of these rules by using the **View** option.

To turn off a Traffic rule temporarily

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Traffic Rules** tab, uncheck the box next to the rule that you want to turn off.
4. Click **Apply**.

Allowing a blocked program

Sometimes the Norton 360 firewall blocks certain programs from accessing the Internet. Such programs might include certain streaming-media programs, network games, or custom business applications that are provided by your employer. If you know that the program's Internet activity is not a threat to your security, you can unblock the program's Internet access.

To allow a blocked program

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Program Rules** tab, select the program that you want to allow access to the Internet.
4. In the **Access** drop-down list for the program entry, click **Allow**.
5. Click **Apply**.

To allow a blocked program from the Security History window

1. In the Norton 360 main window, click **Tasks**.
2. In the **Tasks** window, under **General Tasks**, click **Check Security History**.
3. In the **Security History** window, in the **Show** drop-down list, select **Firewall - Activities**.
4. Select the firewall activity that is associated with the blocked program.
5. Click **More Details**.

6 In the **Security History - Advanced Details** window, under **Actions**, click **Allow**.

Removing a firewall rule

You can remove some of the firewall rules if necessary. However, you cannot modify some of the default Traffic rules that appear in the list. You can view the settings of these rules by using the **View** option.

Do not remove a default firewall rule unless you are an advanced user. Removing a default firewall rule can affect firewall functionality and reduce the security of your computer.

To remove a Traffic rule

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Traffic Rules** tab, select the rule that you want to remove.
4 Click **Remove**.
5 In the **Confirmation** dialog box, click **Yes**.

To remove a Program rule

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Program Rules** tab, in the **Program** column, select the program that contains the rule that you want to remove.
4 Click **Modify**.
To remove all the program rules that are associated with the program, click **Remove**.
5 In the **Rules** window, select the rule that you want to remove.
6 Click **Remove**.
7 In the **Confirmation** dialog box, click **Yes**.
8 Click **OK**.

About Norton Firewall Diagnosis

There may be times when firewall may block the network traffic that you want to allow based on its configuration settings. In such cases, you may have issues in accessing the Internet, the Network, or another computer to perform tasks such as sharing resources.

When you experience network connection problems, Norton Firewall acts quickly in identifying the cause of failure and provides its diagnosis. Norton 360 displays the **Firewall Diagnostics Wizard** when you encounter network connection problems.

Norton Firewall Diagnosis is available only in Windows 7.

The Wizard contains the problem diagnosis report that is unique for different cases of network blocks. For instance, a network block can occur in any of the following cases:

- The one click option to stop all network traffic is active
- The uncommon protocol that is handling the traffic is blocked
- The currently active firewall rule is conditioned to block the traffic that you want to allow
- The traffic has violated the process policy of the firewall
- The traffic has violated the traffic policy of the firewall
- The traffic comes from the restricted zone of networks or computers
- The traffic matches an Intrusion Prevention attack signature

You can use the **Firewall Diagnostics Wizard** as a guide to troubleshoot the network connection problem by yourself.

For each case of network block, the Wizard contains the firewall's analysis of the cause and the possible solutions to fix the block.

Norton 360 recommends that you use the **Firewall Diagnostics Wizard** to remove any type of block. The solutions in the Wizard let you analyze the issue and take a suitable action to resolve the problem.

Using the Wizard to troubleshoot the problem has the following advantages:

- It automatically tries to fix the problem by itself
- It lets you modify the settings that are related to the block
- It lets you view the log details related to the network block event
- It provides you the option to turn off firewall as the last means to resolve the issue

About Intrusion Prevention

Intrusion Prevention scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects your computer against most common Internet attacks.

For more information about the attacks that Intrusion Prevention blocks, go to the following URL:

http://www.symantec.com/business/security_response/attacksignatures

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way.

Intrusion Prevention scanning of every request from all the devices that access your computer increases the

scan time which slows down the network speed of your computer. You can reduce the scan time and improve the network speed of your computer by excluding the trusted devices from Intrusion Prevention scanning. If you are sure that a device on your network is safe, you use the **Edit Device Trust Level** window to change the trust level of the device to **Full Trust**. You can then select the **Exclude from IPS scanning** option to exclude these trusted devices from Intrusion Prevention scan.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. Norton 360 runs LiveUpdate automatically to keep your list of attack signatures up to date. If you do not use Automatic LiveUpdate, you should manually run LiveUpdate once a week.

Turning off or turning on Intrusion Prevention notifications

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks. Whether or not you receive notifications, Intrusion Prevention activities are recorded in Security History. The Security History entries include information about the attacking computer and information about the attack.

You can choose whether you want to receive notifications when Intrusion Prevention blocks suspected attacks based on a particular signature.

To turn off or turn on Intrusion Prevention notifications

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Notifications** row, do one of the following:
   - Move the **On/Off** switch to the right to the **Off** position.
   - Move the **On/Off** switch to the left to the **On** position.
4 In the **Settings** window, click **Apply**.

To turn off or turn on an individual Intrusion Prevention notification

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
4 In the **Intrusion Signatures** window, click an attack signature, and then click **Properties**.
5 In the **Signature Properties** window, uncheck or check **Notify me when this signature is detected**.
6 Click **OK**.
7 In the **Intrusion Signatures** window, click **OK**.
8 In the **Settings** window, click **Apply**.

Excluding or including attack signatures in monitoring

In some cases, benign network activity may appear similar to an attack signature. You may receive repeated notifications about possible attacks. If you know that the attacks that trigger these notifications are safe, you can create exclusion for the attack signature that matches the benign activity.

Each exclusion that you create leaves your computer vulnerable to attacks.

If you have excluded the attack signatures that you want to monitor again, you can include them in the list of active signatures.

To exclude attack signatures from being monitored

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
4. In the **Intrusion Signatures** window, uncheck the attack signatures that you want to exclude.
5. Click **OK**.

To include the attack signatures that were previously excluded

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion Signatures** row, click **Configure**.
4. In the **Intrusion Signatures** window, check the attack signatures that you want to include.
5. Click **OK**.

Turning off or turning on AutoBlock

When an attack is detected from a computer, the attack is automatically blocked to ensure that your computer is safe. If a different attack signature is detected from the same computer, Norton 360 activates AutoBlock. The AutoBlock feature blocks all traffic between your computer and the attacking computer for a specific time period. During this period, AutoBlock also blocks the traffic that does not match an attack signature.

You can specify the period for which you want Norton 360 to block the connections from attacking computers. By default Norton 360 blocks all traffic between your computer and the attacking computer for a period of 30 minutes.

AutoBlock stops traffic between your computer and a specific computer. If you want to stop all traffic to and from your computer, you can use the **Block All Network Traffic** option.

If AutoBlock blocks a computer or computers that you need to access, you can turn off AutoBlock.

To turn off or turn on AutoBlock

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
4. In the **Intrusion AutoBlock** window, under **AutoBlock**, do one of the following:
   - To turn off Intrusion AutoBlock, click **Off**.
   - To turn on Intrusion AutoBlock, click **On (Recommended)**, and then in the **AutoBlock attacking computers for** drop-down list, select how long you want to turn on AutoBlock.
5. Click **OK**.

Unblocking AutoBlocked computers

In some cases, benign network activity can appear to be similar to an attack and AutoBlock blocks the network activity automatically to ensure that your computer is safe. The list of computers that AutoBlock has currently blocked may include the computer that you should be able to communicate with.

If a computer that you need to access appears on the list of blocked computers, you can unblock it. You may want to reset your AutoBlock list if you have changed your protection settings. To reset the AutoBlock list, you can unblock all of the computers that are on the list at one time.

To unblock AutoBlocked computers

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
4. In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, do one of the following:
   - To unblock one computer, select its IP address, and then click **Unblock**.
   - To unblock all computers on the AutoBlock list, click **Unblock All**.
5. Click **OK**.

Permanently blocking a computer that has been blocked by AutoBlock

You can permanently block a computer that has been blocked by AutoBlock. The permanently blocked computer is removed from the AutoBlock list and added as a Restricted computer in the Network Security Map of Home Networking.

To permanently block a computer that has been blocked by AutoBlock

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Intrusion Prevention**, in the **Intrusion AutoBlock** row, click **Configure**.
4. In the **Intrusion AutoBlock** window, under **Computers currently blocked by AutoBlock**, click the computer that you want to block permanently.
5. Under the **Action** column, select **Restrict**.
6. Click **OK**.

Turning off and turning on Browser Protection

You can choose whether you want to protect your Web browser by allowing Norton 360 to block unknown programs from accessing your computer.

By default, the **Browser Protection** option is turned on. In this case, Norton 360 proactively blocks new or unknown malware programs before they attack your computer. By protecting your Web browser, Norton 360 secures your sensitive information and prevents the attackers from controlling your system remotely. This feature checks for browser vulnerabilities in Internet Explorer 6.0 or later, Chrome 10.0 or later, or Firefox 3.6 or later browsers.

Always keep the Browser Protection setting turned on to protect your Web browser against attacks by malicious Web sites.

To turn off or turn on Browser Protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, in the **Browser Protection** row, do one of the following:
   - To turn off Browser Protection, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Browser Protection, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**.
5. If you turned off Browser Protection, in the **Protection Alert** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Browser Protection.
6. Click **OK**.

About Intrusion Prevention exclusion list

The Intrusion Prevention System in Norton 360 scans all the network traffic that enters and exits your

computer. When a device on your network requests access to your computer, Intrusion Prevention scans this request to ensure that it is not a virus attack. If the information matches an attack signature, Intrusion Prevention blocks the traffic from the suspicious device and protects your computer. Scanning every request from all the devices that access your computer increases the scan time which slows down the network speed of your computer.

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. You can configure the trust level of a device using the Network Security Map. You can exclude these trusted devices from Intrusion Prevention scan. Excluding Full Trust devices from the Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a device that is set to Full Trust, Norton 360 does not scan any information that is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

When a device on your network attempts to infect your computer, AutoBlock stops all access requests from this device. If you add this device to the Intrusion Prevention exclusion list, Norton 360 removes the device from the exclusion list.

Ensure that the IP address of the devices that are added to Intrusion Prevention exclusion list never changes.

If you find that any of the devices that you excluded from the Intrusion Prevention scan is infected, you can purge the saved exclusion list. When you purge the exclusion list, Norton 360 removes all the trusted devices from the exclusion list.

Removing all devices from Intrusion Prevention exclusion list

If you are sure that a device on your network is safe, you can change the trust level of the device to Full Trust. These trusted devices can be excluded from Intrusion Prevention scan. Excluding Full Trust devices from Intrusion Prevention scan saves the scan time and improves the network speed of your computer. When you exclude a Full Trust device from Intrusion Prevention scan, Norton 360 does not scan any information that is received from this device. The Full Trust devices that are excluded from Intrusion Prevention scan are added to Intrusion Prevention exclusion list.

If you find that any of the devices that you excluded from Intrusion Prevention scan is infected, you can purge the saved exclusion list and remove all the devices.

You can purge the saved exclusion list under the following circumstances:

- Any of the devices that you excluded from Intrusion Prevention scan is infected.
- Any of the devices that you excluded from Intrusion Prevention scan attempts to infect your computer.
- Your home network is infected.

When a device on your network attempts to infect your computer, AutoBlock stops all the access requests from this device. If you add this device to the Intrusion Prevention exclusion list, Norton 360 removes the device from the exclusion list.

When you remove all the devices from the saved exclusion list, Intrusion Prevention scans every request from all the devices that access your computer.

To remove all the devices from the Intrusion Prevention exclusion list

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3 Click the **Intrusion and Browser Protection** tab.
4 Under Intrusion Prevention, in the **Exclusion List** row, click **Purge**.
5 In the confirmation dialog box, click **Yes**.
6 In the **Firewall** settings window, click **Apply**.

About Download Insight

Download Insight provides information about the reputation of any executable file that you download from the supported portals. The reputation details indicate whether the downloaded file is safe to install. You can use these details to decide the action that you want to take on the file.

Some of the supported portals are:

- Internet Explorer (Browser)
- Opera (Browser)
- Firefox (Browser)
- Chrome (Browser)
- AOL (Browser)
- Safari (Browser)
- Yahoo (Browser)
- MSN Explorer (Browser, E-mail & Chat)
- QQ (Chat)
- ICQ (Chat)
- Skype (Chat)
- MSN Messenger (Chat)
- Yahoo Messenger (Chat)
- Limewire (P2P)
- BitTorrent (P2P)
- Thunder (P2P)
- Vuze (P2P)

- Bitcomet (P2P)
- uTorrent (P2P)
- Outlook (E-mail)
- Thunderbird (E-mail)
- Windows Mail (E-mail)
- Outlook Express (E-mail)
- FileZilla (File Manager)
- UseNext (Download Manager)
- FDM (Download Manager)
- Adobe Acrobat Reader (PDF viewer)

Based on the type of portal you use to download your file, Norton 360 does one of the following:

- Analyzes the file based on its reputation details when the download is complete.
- Analyzes the file based on its reputation details when the file is accessed.

Download Insight uses the file analysis results to provide you the reputation details of the file. The basic reputation levels of the files are good, bad, unproven, and poor. Based on the reputation levels, the files can be broadly classified as follows:

Safe	Includes the files that are either Norton trusted or User trusted. Safe files have good reputation levels. These files do not harm your computer. By default, Auto-Protect allows the execution of the safe files.

Unsafe	Includes the files that Norton 360 identifies as a security risk or a threat. Unsafe files are characterized by bad or poor reputation levels and Norton 360 removes them from your computer.
Unknown	Includes the files that are neither safe nor unsafe. Unknown files have unproven reputation. These files might harm your computer. In the case of an unknown file, Download Insight notifies you that it is unsure of the reputation level of the file. You can use the **View Details** link in the notifications to view more details of the file. For unknown files, Norton 360 lets you decide the action that you want to perform on the file. For example, you can run a file, stop the file from running, or remove the file from your computer.

By default, Download Insight lets you install safe files. For files of unknown reputation levels, Download Insight prompts you to select an action that you want to perform on the file. In case of an unsafe file, Download Insight informs you that Norton 360 has detected the file as a threat and has removed the file.

Based on the reputation details that the Download Insight notifications provide for the files that need attention, you can take an action on the file. The **Download Insight** window provides the various options that let you select an action. The options that appear in the window vary depending on the reputation level

of the downloaded file. The following are some of the options that are available in this window:

Run this program	Lets you install the executable program.
Cancel run	Lets you cancel the installation of the executable program.
Remove this file from my system	Lets you remove the file from your computer.

Security History logs details of all events that Download Insight processes and notifies. It also contains information about the safety level of the file and the action that you take on the file, if any. You can view these details in the **Download Insight** category in Security History.

When you turn off Auto-Protect, Norton 360 automatically turns off Download Insight. In this case, your computer is not adequately protected from Internet threats and security risks. Therefore, ensure that you always keep Auto-Protect turned on to protect your computer from security risks.

When Silent Mode is turned on, Norton 360 suppresses the Download Insight notifications.

Turning off or turning on Download Intelligence

Download Insight protects your computer against any unsafe file that you may run or execute after you download it using a supported Web browser. By default, the **Download Intelligence** option is turned on. In this case, Download Insight notifies you about the reputation levels of any executable file that you download. The reputation details that Download Insight provides indicate whether the downloaded file is safe to install.

There may be times when you want to turn off Download Insight. For example, if you want to download an unsafe file. In this case, you must turn off Download Insight so that Norton 360 lets you download the file and does not remove it from your computer.

You can use the **Download Intelligence** option to turn off or turn on Download Insight.

To turn off Download Intelligence

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, in the **Download Intelligence** row, move the **On/Off** switch to the right to the **Off** position.
4. In the **Settings** window, click **Apply**.
5. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Download Insight, and then click **OK**.
6. In the **Settings** window, click **Apply**, and then click **Close**.

To turn on Download Intelligence

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, in the **Download Intelligence** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**, and then click **Close**.

Configuring the Download Insight Notifications option

You can use the **Download Insight Notifications** option to choose when you want Download Insight to display notifications.

By default, the **Download Insight Notifications** option is set to **On**. Based on the type of portal you use to download your file, Norton 360 does one of the following:

- Notifies you each time when you download an executable file.
- Notifies you only when you download a file that is infected with a local virus identification. If the file that you download is infected with a cloud virus identification, Norton 360 removes the file from your computer and notifies you with the threat details.

When the **Download Insight Notifications** option is set to **Risks Only**, Download Insight notifies only when you download an infected or a suspicious executable file.

Setting the **Download Insight Notifications** to **Risks Only** does not turn off analysis of all the other executable files that you download. Whether or not you receive notifications of all files, Security History keeps a record of all the Download Insight activities. You can review the summary of the Download Insight alerts and notifications in Security History.

To configure the Download Insight Notifications option

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.

3 On the **Intrusion and Browser Protection** tab, under **Download Intelligence**, in the **Download Insight Notifications** row, do one of the following:

- To receive Download Insight notifications only for the infected or the suspicious executable files that you download, move the **Download Insight Notifications** switch to the right to the **Risks Only** position.
- To receive Download Insight notifications for all files that you download, move the **Download Insight Notifications** switch to the left to the **On** position.

4 In the **Settings** window, click **Apply**, and then click **Close**.

Configuring the Download Insight Full Report option

The **Download Insight Full Report** option lets you specify when and for what type of file you want to be prompted to select a suitable action. For example, you can specify the type of downloaded files for which Download Insight asks you to decide what to do with the file and how frequently these prompts for a suitable action must appear.

You can use the following options to configure **Download Insight Full Report**:

Always	When you set the **Download Insight Full Report** option to **Always**, Download Insight prompts you for a suitable action in case of safe and unknown files. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has a safe or an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. In the case of unsafe files, Norton 360 identifies them as threats and removes them.

Unproven Only	When you set the **Download Insight Full Report** option to **Unproven Only**, Download Insight prompts you to select a suitable action for unknown files only. In this case, the **Download Insight** window appears whenever you try to launch any downloaded file that has an unknown reputation score. In this window, you can view details about the file and the options that let you select a suitable action for the file. By default, the **Download Insight Full Report** option is set to **Unproven Only**. In this case, Norton 360 allows the execution of the safe files without prompting you for a suitable action. In the case of unsafe files, Norton 360 identifies them as threat and removes them.

Never	When you set the **Download Insight Full Report** option to **Never**, Download Insight does not prompt you to select a suitable action for any type of file that you download. In this case, the **Download Insight** window does not appear whenever you try to launch any downloaded file. In case of unsafe files, Norton 360 identifies them as threat and removes them. The alert messages that you suppress and the activity details can be reviewed at any time in Security History.

To configure the Download Insight Full Report option

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Firewall**.
3. On the **Intrusion and Browser Protection** tab, under **Download Intelligence**, in the **Download Insight Full Report** row, do one of the following:
   - If you want Download Insight to prompt you for a suitable action in case of safe and unknown files, move the **Download Insight Full Report** switch to the **Always** position.
   - If you want Download Insight to prompts you to select a suitable action for unknown files only, move the **Download Insight Full Report** switch to the **Unproven Only** position.
   - If you do not want Download Insight to prompt you to select a suitable action for any type of file, move the **Download Insight Full Report** switch to the **Never** position.

4 In the **Settings** window, click **Apply**, and then click **Close**.

Turning on or turning off Alert on Poor Stability

When you turn on the **Alert on Poor Stability** option, Download Insight prompts you to select a suitable action when you try to download an unstable file.

When you set the **Download Insight Full Report** option to **Never**, Download Insight does one of the following:

- Does not prompt you to select a suitable action for any type of file that you download if the **Alert on Poor Stability** option is turned off. The **Download Insight** window does not appear whenever you try to open any downloaded file.
- Prompts you to select a suitable action when you try to download an unstable file if the **Alert on Poor Stability** option is turned on. Norton 360 identifies unsafe files as security threat and removes them.

By default, the **Alert on Poor Stability** option is turned off.

To turn on or turn off Alert on Poor Stability

1 In the Norton 360 main window, click **Settings**.
2 On the **Intrusion and Browser Protection** tab, under **Download Intelligence**, in the **Alert on Poor Stability** row, do one of the following:
   - To turn on **Alert on Poor Stability**, move the **On/Off** switch to the left to the **On** position.
   - To turn off **Alert on Poor Stability**, move the **On/Off** switch to the right to the **Off** position.
3 Click **Apply**, and then click **Close**.

About Norton AntiSpam

Norton AntiSpam lets you categorize the email messages that you receive in your email programs into spam email and legitimate email. It filters legitimate

email into the Inbox folder and spam email into the Junk folder or the Norton AntiSpam folder.

Norton AntiSpam uses Symantec enterprise-class, spam-filtering technology to classify the spam email messages from legitimate email messages. Norton AntiSpam uses a real-time filter delivery mechanism and filters email messages using various local filters at different levels. The local filters classify the email messages as spam or legitimate. If the local filters classify the email message as legitimate, Norton AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Symantec Web server for additional analysis.

When the email message is classified as spam, Norton AntiSpam changes the subject of the email message and sends it to your email client. The email client identifies the change in the subject of the email message and moves it to the Junk folder or the Norton AntiSpam folder.

The Norton AntiSpam local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as spam or legitimate. For these filters to work efficiently, Norton AntiSpam requires antispam definition updates at regular intervals through LiveUpdate. These updates contain signature information of spam and legitimate email messages. The updates also contain any new rule that Symantec creates to filter spam email messages.

Norton AntiSpam uses predefined email rules and the user-defined Allowed List and Blocked List, to expedite the scanning of email. It accepts email messages from the list of allowed email senders and blocks email messages from the list of blocked email senders.

Norton AntiSpam also automatically imports the lists of addresses from supported email programs during the initial integration. It helps you keep your list of allowed and blocked email senders in sync with your current address books. When Norton AntiSpam imports

the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Turning off Norton AntiSpam increases your exposure to receive unsolicited email messages. Always ensure that Norton AntiSpam is turned on. It secures your email client from unwanted online content.

You can review all the antispam statistics under the **AntiSpam** category in the **Security History** window.

About spam filtering features

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

Norton 360 provides several powerful features to reduce your exposure to unwanted online content.

Integration with email programs	Adds several options to the toolbar in supported email programs. See "About your email program toolbar" on page 284.

Allowed and Blocked Lists	■ Uses a user-defined address list to expedite the scanning of email. ■ Accepts all email messages from senders in the Allowed List. ■ Treats all email messages from senders in the Blocked List as spam. ■ Allows and blocks email messages from entire domains as well as individual email addresses. See "About Norton AntiSpam settings" on page 515.
Automatic import of addresses	Automatically imports lists of addresses from supported email programs to keep your list of allowed email senders and blocked email senders in sync. See "Identifying authorized senders" on page 287.
Web Query	Lets you query the Symantec Web servers to filter the spam email messages which the local filters fail to classify as spam. See "About Web Query" on page 292.
Automated update of spam definitions	Updates the copies of Symantec spam definition files automatically.

Configuring Client Integration

The Client Integration tab lists the supported email programs, or clients, that are installed on your computer and their associated address books. When you select an email program, Norton 360 adds a **Norton AntiSpam** drop-down list or a few options to the toolbar of the supported email program. You can use

the **Norton AntiSpam** drop-down list or the options to classify the email messages as spam or legitimate. You can also use these options to empty the spam folder and to open the **Settings** window to configure the Norton AntiSpam settings. If your email program does not have a Junk folder, it also adds a Norton AntiSpam folder in the folders area. You can use the Norton AntiSpam folder to sort and store spam messages. However, if your email client has a Norton AntiSpam folder from the previous version of Norton 360, Norton AntiSpam uses the Norton AntiSpam folder and not the Junk folder.

The following email clients do not support client integration:

- Outlook 2010 64-bit
- Thunderbird
- Windows Mail

When you classify an email message as spam or legitimate, Norton AntiSpam lets you send the misclassified email message as feedback to Symantec. You can use the **Feedback** option to send the misclassified email message to Symantec for analysis.

You can also import the list of addresses that are present in the supported email program into the Norton AntiSpam Allowed List and Blocked List. Norton AntiSpam automatically adds the new email addresses from the address book of your supported email program once in a day when your computer is idle. However, if you want to manually import addresses, use the **Import** option in the **Allowed List** window.

When you open your email client, the welcome screen appears. If you do not want the welcome screen to appear in the future, check the **Don't show this again** option before you click **Close**. Norton 360 notifies the successful integration of Norton AntiSpam with your email client.

Norton AntiSpam also automatically imports the lists of addresses from the supported email programs during

the initial client integration. It helps you keep your list of allowed and blocked email senders in sync with your current address books. When Norton AntiSpam imports the addresses from your Outlook address book or Windows address book, it also imports the addresses that are available in the Safe Sender and the Blocked Sender lists.

Norton 360 supports Norton AntiSpam integration with the following email programs:

- Microsoft Outlook 2002/2003/2007/2010
- Outlook Express 6.0 or later

Norton 360 supports only the 32-bit version of Microsoft Outlook 2010.

After successful integration, Outlook Express restarts automatically.

To configure Client Integration

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Client Integration** tab, turn on or turn off the programs with which you want Norton AntiSpam to integrate.
4. Select one or more address books to be imported automatically into your Allowed List.
5. Click **Apply** to save the changes.

About your email program toolbar

Norton AntiSpam adds a drop-down list or a few options to the toolbar of supported email programs.

You can use the following options:

This is Spam	Marks the selected email as spam and moves the email message into the Junk folder or the Norton AntiSpam folder. When you reclassify an email message as spam, Norton 360 provides you the option to send the misclassified email message as feedback to Symantec. This option appears only if the **Feedback** option on the **Client Integration** tab, in the **AntiSpam** settings window, is set as **Ask Me**. When you reclassify an email message as spam, Norton 360 displays a message whether or not to add the sender's email address to the Blocked List. This message appears depending on the option that you select in the drop-down list present at the bottom of the **Blocked List** window.
This is not Spam	Marks the selected email as allowed (not spam) and moves the email message into the **Inbox**. When you reclassify an email message as legitimate, Norton 360 provides you the option to send the misclassified email message as feedback to Symantec. This option appears only if the **Feedback** option on the **Client Integration** tab, in the **AntiSpam** settings window, is set as **Ask Me**. When you reclassify an email message as legitimate, Norton 360 displays a message whether or not to add the sender's email address to the Allowed List. This message appears depending on the option that you select in the drop-down list present at the bottom of the **Allowed List** window.
Empty Spam Folder	Removes all email that has been placed in the Junk folder or the Norton AntiSpam folder.

Open Norton AntiSpam	Displays the Norton AntiSpam settings section of the **Norton 360 Settings** window

Setting Address Book Exclusions

When you add an email address to the Address Book Exclusions list, Norton AntiSpam does not import the address into the Allowed List and Blocked List. If you delete an email address from the Allowed List or Blocked List, Norton AntiSpam automatically adds the address to the Address Book Exclusions list. However, when you delete an email address that you manually added to the Allowed List or Blocked List, Norton AntiSpam does not add the address to the Address Book Exclusions list.

You cannot add a domain name to the Address Book Exclusions list. When you delete a domain name from the Allowed List or Blocked List, Norton AntiSpam does not add the domain name to the Address Book Exclusions list.

You can specify Address Book Exclusions before you import the address book. Add all email addresses to the Address Book Exclusions list that you do not want to import from the address book of your email program.

To add entries to the Address Book Exclusions list

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Filter** tab, in the **Address Book Exclusions** row, click **Configure**.
4. In the **Address Book Exclusions** window, click **Add**.
5. In the **Add Email Address** dialog box, type the email address.
   Optionally, type the name that corresponds to the email address for easy identification.
6. Click **OK** to close the **Add Email Address** dialog box.

7 Click **OK** to save and close the **Address Book Exclusions** window.

To edit or delete entries in the Address Book Exclusions list

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Address Book Exclusions** row, click **Configure**.
4 In the **Address Book Exclusions** window, select the item with which you want to work.
5 Do one of the following:
   - To edit an entry, click **Edit** to open the **Edit Email Address** window, edit the details, and then click **OK**.
   - To delete an entry, click **Remove**.
6 Click **OK** to save and close the **Address Book Exclusions** window.

Identifying authorized senders

If you are sure that an email address or domain is safe and do not want Norton AntiSpam to block them, you can add them to the **Allowed List**

When your computer is idle, Norton AntiSpam automatically imports the address book entries and Safe Sender List entries once in a day.

If you have added a new supported email program, you can import its address book manually to your **Allowed List** immediately or at any time. You can also add names and domains to the **Allowed List** individually.

Before you import the address book, you can specify your Address Book Exclusions. Norton AntiSpam does not import the email addresses that you add to the **Address Book Exclusions** list.

To import an address book

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, click **Import**.
5 In the **Allowed List** window, click **Apply**.
6 Click **OK**.

To add entries to your Allowed List

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, click **Add**.
5 In the **Add Email Address** dialog box, in the **Address Type** drop-down list, select the address type.
You can select one the following options.
   - **Email**
   - **Domain**
6 Do one of the following:
   - To add an email address, type the email address that you want to allow, and optionally, the name of the sender.
   - To add a domain name, type the address of the domain (for example, symantec.com), and optionally, the name of the domain.
7 Click **OK**.
8 In the **Allowed List** window, click **Apply**.
9 Click **OK**

To edit or delete entries in the Allowed List

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.

3 On the **Filter** tab, in the **Allowed List** row, click **Configure**.
4 In the **Allowed List** window, select the item that you want to edit or delete.
5 Do one of the following:
   - To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and click **OK**.
   - To delete an entry, click **Remove**.

     When you delete an entry that was imported, Norton AntiSpam automatically adds it to the Address Book Exclusions list.
6 In the **Allowed List** window, click **Apply**.
7 Click **OK**.

Identifying senders of spam

If you do not want to receive any email messages from a specific address or domain, you can add it to the Blocked List. Norton AntiSpam marks all email messages from this address or domain as spam.

Norton AntiSpam also automatically imports the lists of addresses that are available in the Blocked Sender lists of your email program into the Blocked List during the initial client integration or address book import.

Norton AntiSpam lets you type invalid email addresses to the Blocked List.

Always add suspicious email addresses and domains to the Blocked List, so that you do not receive unsolicited email messages from such addresses or domains.

To import addresses to the Blocked List

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Allowed List** row, click **Configure**.

4 In the **Allowed List** window, click **Import**.
5 In the **Allowed List** window, click **Apply**.
6 Click **OK**.

To add entries to the Blocked List

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Blocked List** row, click **Configure**.
4 In the **Blocked List** window, click **Add**.
5 In the **Add Email Address** dialog box, in the **Address Type** drop-down list, select the address type.
You can select one of the following:
   - **Email**
   - **Domain**
6 Do one of the following:
   - To add an email address, type the email address that you want to block, and the name of the sender.
   - To add a domain, enter the address of the domain (for example, symantec.com), and the name of the domain.
7 Click **OK**.
8 In the **Blocked List** window, click **Apply**.
9 Click **OK**.

To edit or delete entries in the Blocked List

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3 On the **Filter** tab, in the **Blocked List** row, click **Configure**.
4 In the **Blocked List** window, select the item with which you want to work.

5 Do one of the following:
   - To edit an entry, click **Edit** to open the **Edit Email Address** dialog box, edit the details, and then click **OK**.
   - To delete an entry, click **Remove**.

     When you delete an entry that was imported, Norton AntiSpam automatically adds it to the **Address Book Exclusions** list.
6 In the **Blocked List** window, click **Apply**.
7 Click **OK**.

Setting the Feedback option

Email messages in the email client might sometimes get wrongly classified as spam or legitimate. The **Feedback** option lets you send the misclassified email message as feedback to Symantec for analysis.

The **Feedback** option is available only when Microsoft Outlook or Outlook Express is installed on your computer.

To set the Feedback option

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.

3 On the **Client Integration** tab, in the **Feedback** row, select any one from the following three options:

On	Automatically sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Ask Me	Prompts you before Norton AntiSpam sends the misclassified email message to Symantec when you classify an email message as spam or legitimate
Off	Does not send the misclassified email message to Symantec

4 Click **Apply**.

5 Click **Close**.

About Web Query

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images. The Web Query is a feature of Norton AntiSpam that Norton 360 uses to classify the email messages more effectively.

An effective spam filtration is possible when each email message that you receive is scanned through different filters. With only one or two levels of email filters, a high percentage of legitimate emails are misclassified as spam or spam is misclassified as legitimate. To avoid such misclassification, Norton AntiSpam employs different filters. Each email filter uses a unique

approach to filter spam email messages from legitimate email messages.

The email messages that you receive in your email program undergo scanning through different local filters of Norton AntiSpam. The local filters use Whitelist technique, Blacklist technique, and patented filtering technology to classify email messages as legitimate or spam. If the local filters classify an email message as spam, Norton AntiSpam changes the subject of the email message. Norton AntiSpam then sends the email message to your email client. If the local filters fail to classify the email message as spam, Norton AntiSpam collects information such as signature and URL hashes of the email message. Norton AntiSpam then sends this information to the Web Query filter for additional analysis.

The Web Query filter analyzes the signature and URL hashes of the email message and then sends the analysis report to Norton AntiSpam. If the email message is identified as spam, Norton AntiSpam alters the subject of the email message and sends it to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends that you keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

Turning off or turning on Web Query

Norton AntiSpam uses local filters to identify spam email messages. The email messages that the local filters do not identify as spam are then scanned additionally through the Web Query filter. Web Query filter analyzes the signature and URL hashes of the email messages to classify them as legitimate email or spam email.

If the email message is identified as spam, then Norton AntiSpam alters the subject of the email message.

Norton AntiSpam then sends the email message to your email program. Based on predefined email rules, the email program then moves the email message to the Junk folder or the Norton AntiSpam folder.

Symantec recommends you to keep the **Web Query** option turned on. Turning off the **Web Query** option increases your exposure to the spam email messages that contain phishing or spam URLs.

To turn off the Web Query filter

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Filter** tab, in the **Web Query** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**.
5. Click **Close**.

To turn on the Web Query filter

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **AntiSpam**.
3. On the **Filter** tab, in the **Web Query** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**.
5. Click **OK**

About configuring POP3 and SMTP ports

Norton 360 automatically configures your email program to protect it from viruses and other security threats. Norton 360 supports all email accounts that use non-SSL POP3 and SMTP communication protocols. Norton 360 also scans all incoming and outgoing email messages.

Norton 360 lets you manually configure your POP3 and SMTP email ports for email protection. Typically, your Internet service provider (ISP) provides you the port

numbers for your email program. If the SMTP and POP3 port numbers for your email program are different from the default port numbers, you must configure Norton 360.

To ensure email protection, Symantec recommends that you check the POP3 and SMTP port numbers for your email program. If they are not the default ports, add them to the **Protected Ports** window. To configure the **Protected Ports** option, go to the Norton 360 main window, and then click **Settings > AntiSpam > Filter > Protected Ports > Configure**.

If you do not want Norton 360 to protect a port, you can remove the port from the **Protected Ports** window.

You cannot remove the default SMTP port 25 and POP3 port 110. Norton 360 automatically protects these default ports.

Adding POP3 and SMTP ports to Protected Ports

Norton 360 supports all email programs that use POP3 and SMTP communication protocols with default ports. However, if your email program is not configured with the default ports, you can manually configure your POP3 and SMTP email ports.

To ensure email protection, the POP3 and SMTP port numbers must be protected. If the POP3 and SMTP port numbers are not the default ports, Symantec recommends that you add the port numbers to the **Protected Ports** window.

To add POP3 and SMTP ports to Protected Ports

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, click **AntiSpam**.
3. On the **Filter** tab, in the **Protected Ports** row, click **Configure**.
4. In the **Protected Ports** window, click **Add**.

5 In the **Add Port to protect** window, in the **Port Type** drop-down list, do one of the following:
   - To add the incoming email port, click **POP3**.
   - To add the outgoing email port, click **SMTP**.
6 In the **Port** box, type the port number.
   The port number must be between 1 and 65535.
7 Click **OK**.
8 In the **Protected Ports** window, click **Apply**, and then click **OK**.
9 In the **Settings** window, click **Close**.

Removing an email port from Protected Ports

If you do not want Norton 360 to protect a port, you can remove the port from the **Protected Ports** window.

Norton 360 automatically protects the default SMTP port 25 and the default POP3 port 110. You cannot remove these default ports.

To remove an email port from Protected Ports

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, click **AntiSpam**.
3 On the **Filter** tab, in the **Protected Ports** row, click **Configure**.
4 In the **Protected Ports** window, click the port that you want to remove, and then click **Remove**.
5 Click **Apply** and then click **OK**.
6 In the **Settings** window, click **Close**.

About Metered Broadband Mode

The Metered Broadband Mode feature lets you set up policies to restrict the Internet usage of Norton 360. You can define the amount of network bandwidth that Norton 360 can use.

You can choose a communication policy that suits your Internet connection. If you have unlimited Internet

plan, you can set up **No Limit** policy so that Norton 360 connects to Symantec servers to ensure complete protection. However, if you think that Norton 360 uses too much of your Internet connection, you can restrict the Internet usage of Norton 360. Metered Broadband Mode helps you manage the data transfer between Norton 360 and your adapter.

To connect to the Internet, Norton 360 accesses the gateway through an adapter. The adapter is present either on your computer or on a connecting device. The connecting device can be a 3G phone, an Internet data card, or a wireless network card. Metered Broadband Mode lets you set up a policy for each adapter that Norton 360 uses to connect to the Internet.

You can set up one of the following policies for each of the adapter that Norton 360 uses to connect to the Internet:

- **No Limit**

  Lets Norton 360 use the network bandwidth that is required to ensure complete protection. Symantec recommends that you apply this policy.
- **Critical Updates Only**

  Lets Norton 360 access the Internet only to receive critical product updates or virus definitions. If you have a limited Internet connection, you can select the **Critical Updates Only** option to ensure protection from different security threats.
- **No Traffic**

  Lets you block Norton 360 from connecting to the Internet. If you choose this policy, Norton 360 cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.

Turning off or turning on Metered Broadband Mode

You can set up policies to restrict the Internet usage of Norton 360. If you do not want to restrict the

Internet usage of Norton 360, you can turn off **Metered Broadband Mode**.

If you feel that Norton 360 uses too much network bandwidth, you can turn on **Metered Broadband Mode**. Then, you can set up policies to restrict the Internet usage of Norton 360. Norton 360 connects to the Internet based on the policy that you set up in the **Metered Network Settings** window. By default, **Metered Broadband Mode** is turned on.

To turn off Metered Broadband Mode

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Metered Broadband Mode** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**.
5. Click **Close**.

To turn on Metered Broadband Mode

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Metered Broadband Mode** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**.
5. Click **Close**.

Defining the Internet usage of Norton 360

If you think that Norton 360 uses too much of your network bandwidth, you can restrict the Internet usage of Norton 360. You can set up policy for each adapter that Norton 360 uses to connect to the Internet.

The **Metered Network Settings** window lists all the adapters that your computer uses to connect the Internet. You can view the status of the adapters that are currently in use. The network policy that you set

up defines the amount of network bandwidth that Norton 360 can use.

To define the Internet usage of Norton 360

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Metered Broadband Mode** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Configure**.
   The **Metered Network Settings** window lists all the adapters that Norton 360 uses to connect to the Internet.
5. Under the **Policy** column, click the drop-down list next to the adapter for which you want to set up a policy.
6. Select one of the following:
   - **No Limit**

     Lets Norton 360 use the network bandwidth that is required to ensure complete protection.
   - **Critical Updates Only**

     Lets Norton 360 access the Internet only to receive critical product updates or virus definitions.

     If you have a limited Internet connection, you can select the **Critical Updates Only** option to ensure protection from different security threats.
   - **No Traffic**

     Lets you block Norton 360 from connecting to the Internet. If you choose this policy, Norton 360 cannot receive critical virus definitions and program updates, which can lead to potential dangers and virus attacks.
7. Click **Apply**, and then click **OK**.
8. In the **My Network** settings window, Click **Close**.

Securing your sensitive data

9

This chapter includes the following topics:

- About securing your sensitive data

About securing your sensitive data

The Internet provides the fastest and the easiest way to exchange information. In spite of the many advantages that the Internet provides, you are vulnerable to information theft and identity theft. Information can be stolen and misused in several ways.

Following are a few of the most common methods of information theft:

- Online financial transactions
- Unsafe online storage of sensitive information
- Misuse of your identity while you communicate online

The Identity Safe feature in Norton 360 offers several powerful ways to tackle identity theft. Identity Safe is the best tool that you can use to safeguard your identity while you are online.

About Safe Surfing

Safe Surfing comprises of the Antiphishing and the Norton Safe Web features. Antiphishing analyzes the security level of the Web sites that you visit and displays the results in the **Norton Site Safety** pop-up

window. The Norton Safe Web feature provides you a safe search environment in the Web by displaying the site rating icons next to every search result.

When you install Norton 360, it adds the **Norton Toolbar** to the Internet Explorer, Firefox, or Chrome browsers. Norton 360 protects your Web browsers when you turn on the Antiphishing and Norton Safe Web options in the **Safe Surfing** section under Identity Safe option of the Norton 360 **Settings** window.

The Antiphishing and Norton Safe Web features are supported in the Internet Explorer, Firefox, or Chrome Web browsers.

When you turn off Antiphishing and Norton Safe Web, Identity Safe may autofill fraudulent Web sites with your confidential information. Symantec recommends that you do not browse the Web when Antiphishing and Norton Safe Web features are turned off.

About Antiphishing

Antiphishing protects you from visiting unsafe Web sites. When Antiphishing is turned on, the Antiphishing component analyzes the security level of the Web sites that you visit. It then displays the results in the **Norton Site Safety** pop-up window. Antiphishing also blocks navigation to the Web sites that are confirmed to be fraudulent.

Antiphishing provides you the following information about the Web sites you visit:

- If the Web site is safe to enter confidential information
- If the Web site is fraudulent
- If the Web site is suspicious
- If the Web site is known to give annoying results

The **Norton Site Safety** pop-up window in Internet Explorer, Firefox, or Chrome Web browsers lets you view more details about the safety status of the Web sites you visit.

In addition, the **Norton Site Safety** pop-up window includes information about Symantec Authenticated Web sites. Web site hackers often mimic company Web sites to create fraudulent Web sites. Norton 360 identifies the fraudulent Web sites.

Symantec analyzes the pages of these sites and verifies if they belong to the company that it represents. You can be confident that the information that you provide goes to the company with which you want to do business.

You can report the evaluation of a Web site you suspect to be fraudulent to Symantec for further evaluation. Use the **Report Site** option from **Norton Toolbar** to report a Web site. You can also report the evaluation of a Web site that you suspect to be fraudulent but Antiphishing reports as safe.

Even when you turn off the **Antiphishing** option, Norton 360 protects you from Internet threats through its Norton Safe Web features. When Antiphishing is turned off, you cannot use the **Report Site** option in the **Norton** menu to submit the evaluation of the Web site to Symantec.

The **Norton Site Safety** pop-up window displays the following messages:

- **Site is Safe**
- **Site is Unsafe**
- **Site Untested**
- **Norton Secured**
- **Caution**
- **Fraudulent Site**
- **Suspicious Site**
- **Page Not Analyzed**

Turning off or turning on Antiphishing

Antiphishing protects you from visiting unsafe Web sites. The Antiphishing feature in Norton 360 analyzes

the security level of all the Web sites that you visit and displays the results in the **Norton Site Safety** pop-up window. Antiphishing also blocks navigation to the Web sites that are confirmed to be fraudulent.

The **Norton Site Safety** pop-up window helps you understand if the Web site that you visit is safe or unsafe.

You can turn off or turn on Antiphishing in the **Safe Surfing** section of the **Identity Protection** settings window.

To turn off or turn on Antiphishing

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. In the **Antiphishing** row, do one of the following:
   - To turn off Antiphishing, in the **Antiphishing** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Antiphishing, in the **Antiphishing** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

Reporting an incorrect evaluation of a Web site

On rare occasions, Antiphishing may report incorrect evaluation of a Web site. For example, you might visit a site that you shop with regularly and Antiphishing reports that the site is fraudulent. On the contrary, you might visit a Web site that you suspect is a phishing site, but Antiphishing reports that no fraud was detected. In either case, you can report the Web site to Symantec for further evaluation.

The Web site you want to report to Symantec for further evaluation must be kept open in your Web browser.

To report an incorrect evaluation of a suspicious Web site

1. Open your browser and go to the Web site that you think is suspicious.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Report site**.
3. In the dialog box that appears, verify that the Web site address and click **Submit**.
4. In the confirmation dialog box, click **Close**.

To report an incorrect evaluation of a safe Web site

1. Open your browser and go to the Web site that you think is safe.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Report site**.
3. In the dialog box that appears, verify that the Web site address and click **Submit**.
4. In the confirmation dialog box, click **Close**.

About Norton Safe Web

Norton Safe Web helps you surf, search, and shop more safely on the Internet. By using Norton Safe Web, you can check if a Web site is malicious or not even before you visit it. Norton Safe Web analyzes the Web sites you visit and detects if there are any viruses, spyware, malware, or other security threats that exist on the Web sites. Based on the analysis, Norton Safe Web provides safety ratings for all the Web sites.

In addition, Norton Safe Web lets you view the community rating and user reviews of the Web sites you visit.

Norton Safe Web supports Internet Explorer, Firefox, or Chrome Web browsers.

You can view the site safety status of any Web site using the **Full Report** option on the **Norton Site Safety** pop-up window. You can also use the **Community Buzz** option on the **Norton** menu to view the safety status of the Web sites.

The **Community Buzz** option is available only in English-language versions of Windows.

For each Web site that you want to know the site safety status, Norton Safe Web lets you do the following:

- View the Norton rating.
- View the community rating.
- Add your reviews.
- View the user reviews.
- View a list of keywords that are tagged to the Web site.
- View the threat information and the general information about the Web site.

If you use a proxy server to connect to the Internet, you must configure the Network Proxy Settings of Norton 360.

When you search the Internet using Google, Yahoo, or Bing search engines, Norton Safe Web displays site rating icons next to the search results. As you move the mouse pointer over the Norton icon, a pop-up appears with site safety and shopping safety information. The pop-up displays brief information about the safety of the site. Norton Safe Web also provides a detailed report about the safety of the Web Sites you visit.

You can click the icon next to the search results or the **Full Report** option in the **Norton Site Safety** pop-up window to view the detailed report. The report is displayed on the Norton Safe Web site.

Norton Safe Web provides the following Web site safety states when you browse through the Internet:

Norton Secured	You can see Norton Secured icon next to the search results. Symantec has analyzed this page and determined that the Web site is VeriSign trusted and is safe to visit.
Site is Safe	You can see a green OK icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that it is safe to visit.
Site Untested	You can see a gray question mark icon next to the search results. When you visit this Web site, the **Norton Toolbar** shows a green OK icon. Norton Safe Web has not analyzed this Web site and it does not have sufficient information about this web site. As Symantec has not tested the Web site, it is recommended that you do not visit this Webs site.

Site is Unsafe	You can see a red cross (x) icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that the Web site is unsafe to visit. This Web site may attempt to install malicious software on your computer.
Caution	You can see a yellow exclamation mark icon next to the search results. When you visit a Web site with this status, you can see a similar status icon on the **Norton Toolbar**. Norton Safe Web has analyzed this Web site and determined that this web site has some threats that are classified as **Annoyance Factors**. These annoyance factors are not dangerous, but it can install unwanted applications on your computer without your permission.

In addition to the site safety information, Norton Safe Web provides the following shopping safety information:

Safe	Norton Safe Web has analyzed this Web site and determined that you can have a safe shopping experience.

Untested	Norton Safe Web does not have sufficient information about this Web site to provide a shopping safety rating.
Risky	Norton Safe Web has analyzed this Web site and determined that the site has shopping risks. Symantec recommends that you do not visit this page. The Web site may sell counterfeit items without proper indication.
Limited	Norton Safe Web has analyzed this Web site and has only some information about the Web site to provide shopping safety information. The information is not sufficient to declare that the Web site is safe to shop.

When you visit any Web site that has an unsafe status, Norton Safe Web blocks that Web page. If you still want to view the site, use the **Continue to site anyway** option that appears on the blocked page. You can use the **Malicious Site Warning Page** option under **Safe Surfing** section of the Identity Protection settings to turn off or turn on this setting. If you turn off this option, Norton Safe Web does not block the unsafe Web sites. However, **Norton Toolbar** still displays the status of these sites as unsafe even when the option is turned off.

In addition, Norton Safe Web protects your computer while you use Facebook. It scans each URL that is available on your Facebook Wall and displays the Norton rating icons for the scanned URLs. You can also let other Facebook users know about the security status of any Web site.

To scan your Facebook Wall using Norton Safe Web, use the **Scan Facebook Wall** option. The option appears when you click the **Run Scans** option in the **Tasks** window.

Turning off or turning on Norton Safe Web

Norton Safe Web protects your computer while you browse the Internet using Internet Explorer, Firefox, or Chrome Web browsers. It analyzes the security levels of the Web sites that you visit and indicates if the Web sites are free from threats. It provides you a safe environment on the Web by displaying the site rating icons next to each search result. The site rating icons lets you know if a Web site is malicious or not even before you visit it.

You can turn off or turn on Norton Safe Web in the **Safe Surfing** section under **Identity Protection** settings window.

To turn off or turn on Norton Safe Web

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. In the **Norton Safe Web** row, do one of the following:
   - To turn off Norton Safe Web, in the **Norton Safe Web** row, move the **On/Off** switch to the right to the **Off** position.
   - To turn on Norton Safe Web, in the **Norton Safe Web** row, move the **On/Off** switch to the left to the **On** position.
4. In the **Settings** window, click **Apply**.
5. Click **Close**.

Searching the Web using Norton Safe Search

Norton Safe Search enhances your Web search experience. When you search the Internet using Norton Safe Search, it uses Ask.com to generate the search results. Norton Safe Search provides the site safety

status and Norton rating for each of the search results generated.

By default, the **Norton Safe Search** box is disabled. After you install Norton 360 and open Internet Explorer, Firefox, or Chrome Web browsers for the first time, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search.

Norton Safe Search provides you the intelligent search-as-you-type feature that displays search suggestions when you type a few letters of the search phrase.

In addition, Norton Safe Search provides the following features:

Unsafe Site Filter	When you search the Internet using Norton Safe Search, it analyzes the security levels of the Web sites and displays the search results. You can use the **Filter Out Unsafe Sites** option in the Norton Safe Search Web site to filter the unsafe Web sites from the search results. When you click the **Filter Out Unsafe Sites** option the **Unsafe Site Filter** option is turned on. By default this option is turned off.

Erase Search History	Norton Safe Search enables you to erase all the data that are related to your search activities from the Ask.com server. The Privacy Safeguard feature of Norton Safe Search removes the search data, such as your IP address, user identifier, and session identifier from the Ask.com server. You can turn on or turn off Privacy Safeguard using the **Turn On Privacy Safeguard** and **Turn Off Privacy Safeguard** options respectively.

Norton Safe Search feature is available only for some regions including the United States, the United Kingdom, Canada, Australia, and Germany. The Privacy Safeguard feature is available only for the United States, the United Kingdom, and Canada.

You can use Norton Safe Search even when you turn off the Identity Safe features.

Norton Safe Search is supported only in the Internet Explorer, Firefox, or Chrome Web browsers.

To search the Web using Norton Safe Search

1. Start your Web browser.
2. On the **Norton Toolbar**, in the **Norton Safe Search** box, type the search string that you want to search.
3. Do one of the following:
   - Click **Search**.
   - In the pop-up window that appears, select a search suggestion that matches your search string.

About Identity Safe

Identity Safe helps you manage your identities and provides additional security while you perform online transactions.

The following features in Identity Safe provide secure storage of your sensitive information:

Edit Logins	Stores login information, such as your login credentials for your online bank account, email user ID, and password.
Edit Cards	Stores your personal information, such as addresses, date of birth, and credit card information.
Edit Notes	Stores the details, such as passport numbers and social security numbers.

In addition to being a depository of sensitive information, Identity Safe provides the following features:

- Protects you from identity theft when you perform online transactions

  Antiphishing also helps to protect you from malicious Web sites when you perform online transactions.
- Manages your card information when you have multiple credit cards to maintain
- Safeguards the data that you save on your computer

  By saving your data with a local vault, you can prevent your sensitive Identity Safe data on your computer from being misused. A local vault is specific to each of the Windows user accounts present on your computer.

- Provides you the ease of carrying and using your Identity Safe data when you are on the move

  By saving your data using an online vault, you can access your sensitive Identity Safe data from any computer that has Norton 360 installed.

Norton 360 adds the **Norton Toolbar** to the Internet Explorer, Firefox, or Chrome Web browsers. The **Norton Toolbar** has the following components:

- **Norton** menu
- **Norton Safe Search**
- **Safe Web** indicator
- **Identity Safe** menu

When you have cards or logins in Identity Safe, the **Identity Safe** menu displays the list of cards and logins.

Norton 360 supports Google Chrome version 10.0 or later.

If you turn off Identity Safe, you cannot access your logins and Identity Safe features from the **Norton Toolbar**.

Norton 360 lets you view and access some of the Identity Safe features even after the product expires. This way, you can still view your login details even after Norton 360 expires. However, it is not safe to browse the Internet after Norton 360 expires as you are vulnerable to online thefts and phishing attacks.

When your product expires, you cannot access the Identity Safe features from the **Identity Protection** section of the **Settings** window. You can view and access these features using the **Identity Safe** menu or the **Norton** menu that is available on the **Norton Toolbar**.

The following are the activities that you can perform after the product expires:

- Back up your Identity Safe data and save it as a .DAT or .CSV files.

- Open the **Edit Logins** window and view the logins that you saved.

About setting up Identity Safe

Identity Safe helps you manage your sensitive information and provide additional security while you perform online transactions. The features in Identity Safe provide a secure storage for your personal information such as your address, login information, passwords, and credit card details.

Identity Safe provides a secure storage for the following:

- Login information such as user IDs and passwords of your email accounts
- Personal information such as your address, date of birth, passport number, and social security number.
- Credit card details including card number and card expiry date.

You can view all the options that are available in Identity Safe only after you set up Identity Safe.

For each Windows user account, Identity Safe lets you create a local vault and save your Identity Safe data. The data that you save and any of the Identity Safe settings that you configure are specific to that local vault. You cannot access the data that you save in one Windows user account from another user account. This way Identity Safe protects your sensitive data from being misused even when you share your computer with others.

In addition to the local vault that you create on a Windows user account, you can save your Identity Safe data in online vault.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton 360 must be installed.
- The computer must be connected to the Internet.

The Identity Safe data is stored online using your Norton Account. You can create only one online vault for a Norton Account.

If you have Identity Safe data that is stored on any external drives from the older versions of Norton 360, you can convert that portable profile to local vault or online vault. When you connect your external drive to your computer, the Identity Safe menu in the **Norton Toolbar** provides option to merge or delete the Identity Safe data from your portable profile. You can merge the data from the portable profile to local vault or online vault.

Turning off or turning on Identity Safe

Identity Safe helps you manage your identity and provides additional security while you perform online transactions. You can use the various features in Identity Safe to manage your personal data such as addresses, date of birth and credit card information. The logins, cards, and notes help you store and use your personal information in a secure way.

You can turn off or turn on the Identity Safe from the **Quick Controls** in the **Settings** window or from the **Settings** window for **Identity Protection**.

After you turn on Identity Safe, you must log in to Identity Safe to access the various features.

To turn off or turn on Identity Safe from Quick Controls

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, do one of the following:
   - To turn off Identity Safe, uncheck **Identity Safe**.
   - To turn on Identity Safe, check **Identity Safe**.

To turn off Identity Safe from Settings window

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.

2 In the **Identity Protection** settings window, in the **Identity Safe** row, move the **On/Off** switch to the right to the **Off** position.

3 Click **Apply**.

To turn on Identity Safe from Settings window

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.

2 In the **Identity Protection** settings window, in the **Identity Safe** row, move the **On/Off** switch to the left to the **On** position.

3 Click **Apply**.

About Identity Safe vaults

You can create one local vault for each Windows user account on your computer. The data that you save and the Identity Safe settings that you make are specific to that local vault. You cannot access the data that you save in one Windows user account from another Windows user account. This way Identity Safe protects your sensitive data from misuse by multiple users of your computer.

Symantec recommends that you create separate password-protected Windows user accounts if you want to share your computer with multiple users.

In addition to the local vault that you create on a Windows user account, you can save your Identity Safe data in online vault. When you move your Identity Safe data from local vault to online vault, the data in your local vault is permanently removed. The Identity Safe data is stored online using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton 360 must be installed.
- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account.

If you have Identity Safe data that is stored on any external drives from the older versions of Norton 360, you can convert that portable profile to local vault or online vault. When you connect your external drive to your computer, the **Identity Safe** menu in the **Norton Toolbar** provides option to merge the Identity Safe data from your portable profile. You can merge the data from the portable profile to your local vault or online vault.

In addition to the features such as saving logins, cards, and notes, you can do the following using your Identity Safe vault:

- Import your Identity Safe data from the file you already backed up. You can also import the data that you stored in portable profile from an older version of the product to the current version.
- Export your Identity Safe data to .DAT file.
- Reset your Identity Safe.

About creating Identity Safe vaults

Identity Safe helps you manage your sensitive information and provide additional security while you perform online transactions. The various features in Identity Safe provide a secure storage for your personal information such as your address, login information, passwords, and credit card details.

Identity Safe lets you create one local vault per Windows user account.

In addition to the local vault, you can save your Identity Safe data in online vault. When you move your Identity Safe data from local vault to online vault, the data in your local vault is permanently removed.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton 360 must be installed.
- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account. You must log in to your Norton Account to move Identity Safe data from the local vault to the online vault.

You can create Identity Safe vaults from the **Identity Safe** section under **Identity Protection** of the **Settings** window.

Creating local vault and online vault

Identity Safe lets you create a local vault and save your Identity Safe data. You can create one local vault for each Windows user account.

In addition to the local vault that you create on a Windows user account, you can save your Identity Safe data in online vault. The Identity Safe data is stored online vault using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton 360 must be installed.
- The computer must be connected to the Internet.

You can create only one online vault for a Norton Account.

To create local vault

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
4. In the **Set Up Identity Safe** window, in the **Create Password** box, type your password.
5. In the **Confirm Password** box, type the password again to confirm.
6. In the **Password Hint** box, type a hint for the password.

7 Uncheck **Store information online through your Norton Account**.
This option appears only if you log in to your Norton Account.

8 Click **Create**.

9 In the **Identity Safe Setup Successful** window, click **Done**.

To create online vault

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.

3 Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.

4 Click **Login to Norton Account**, and enter your Norton Account credentials. If you do not have a Norton Account, you can create a new Norton Account using **Create Norton Account** option in the **Login to Norton Account** window.

5 In the **Set Up Identity Safe** window, in the **Create Password** box, type the password.
You must provide a strong password to create online vault. You can click **How to create a strong password?** link to know more about creating strong passwords.

6 In the **Confirm Password** box, type the password again to confirm.

7 In the **Password Hint** box, type a hint for the password.

8 Check **Store information online through your Norton Account**.
This option appears only if you log in to your Norton Account.

9 Click **Create**.

10 In the **Identity Safe Setup Successful** window, click **Done**.

Logging in to Norton Account

Identity Safe lets you create a local vault and an online vault to save your Identity Safe data. You must log in to your Norton Account to create an online vault. The Identity Safe data is stored online using your Norton Account.

You can access the Identity Safe data that you stored online from any computer that meets the following criteria:

- The latest version of Norton 360 must be installed.
- The computer must be connected to the Internet.

You can create only one online vault per Norton Account. If you already have a Norton Account, you can log in with your credentials or create a new account.

To log in to Norton Account

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
4. At the bottom of the **Set Up Identity Safe** window, click **Login to Norton Account**.
5. In the **Login to Norton Account** window, type your **E-mail Address** and **Password**.
6. Click **Log In**.

Moving local vault to online vault

You can move the Identity Safe data from your local vault to the online vault. When you move the data from your local vault to online vault, all the data in your local vault is removed permanently.

The **Move Identity Safe Online** option in Identity Safe helps you to save your data online.

The following are the benefits of moving your Identity Safe data online:

- Lets you access your Identity Safe data from any computer.

  Your computer must have the latest version Norton 360 installed and must be connected to the Internet.

- Lets you access your Identity Safe data from online vault without depending on any external drive.
- Provides a convenient means to automatically synchronize Identity Safe data across different computers using your Norton Account.

You must log in to your Norton Account to move the Identity Safe data from your local vault to online vault.

To move local vault to online vault

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. Under **Identity Safe**, in the **Move Data Online** row, click **Configure**.
4. In the **Move Identity Safe Data Online** window, in the **Enter the Password** box, type the password for your local vault.
5. Click **Login to Norton Account**.
6. In the **Login to Norton Account** window, type your Norton Account user name and password, and click **Log In**.
7. Click **Validate**.
8. In the **Move Identity Safe Data Online** window, click **Move Data**.
9. In the **Move Identity Safe Data Online** window, click **Done**.

Merging local vault to online vault

Identity Safe lets you store and manage your sensitive information including your address, login information, passwords, and credit card details. You can create a

local vault and save your Identity Safe data in your local computer.

In addition to the local vault that you create, you can save your Identity Safe data in an online vault. When you save your data in online vault, you can access your Identity Safe data from any computer that has Norton 360 installed.

You can merge the Identity Safe data from your local profile that you have created into your online vault.

When you merge the data from local vault to online vault, the data from the local vault is permanently moved to the online vault. You can access the data from the online vault.

To merge local vault to online vault

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. Under **Identity Safe**, in the **Move Data Online** row, click **Configure**.
4. In the **Move Identity Safe Data Online** window, in the **Enter the Password** box, type the password for your local vault.
5. Click **Login to Norton Account** option at the bottom of the **Move Identity Safe Data Online** window.
6. In the **Login to Norton Account** window, type your Norton Account user name and password, and click **Log In**.
7. Click **Validate**.
   If you already have an online vault, Norton 360 automatically takes you to **Merge Identity Safe Online** window to merge your local vault with your online vault.
8. In the **Warning** dialog box, click **Yes**.
   This window appears only if your Norton Account already has an online vault associated with it.

9 In the **Merge Identity Safe Data Online** window, type your online vault password associated with your Norton Account in the **Enter the Password** box.

10 In the **Merge Identity Safe Data Online** window, click **Merge**.

Deleting local vault and online vault

Identity Safe lets you create a local vault and an online vault to save your Identity Safe data. If you no longer require your Identity Safe data that is stored in your local vault and online vault, you can delete the vaults. When you delete the local vault and online vault, all the Identity Safe data is permanently removed.

To delete the local vault and online vault

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.

3 Under **Identity Safe**, in the **Delete Data** row, click **Configure**.

4 In the **Warning** window, click **Yes**.

5 In the **Settings** window, click **Apply**.

6 Click **Close**.

Merging portable profile to local vault or online vault

If you have Identity Safe data that is stored on any external drives from the older versions of Norton 360, you can merge that portable profile to local vault or online vault. When you connect your external drive to your computer, the **Identity Safe** menu in the **Norton Toolbar** provides option to merge the Identity Safe data from your portable profile. You can merge the data from the portable profile to local vault or online vault.

You can merge the Identity Safe data from the portable profile to the vault that you are currently logged in.

To merge the Identity Safe data from portable profile to local vault or online vault

1. On the **Norton Toolbar**, in the **Identity Safe** menu, click **Merge Portable Data (Drive:\)**.
   This option appears only if you connect an external drive with portable profile.
2. In the dialog box that appears, click **Yes**.
3. In the **Import Identity Safe Data** window, under **Import my data from**, click **Portable Profile (Drive:\)**.
4. In the **Password** box, type the password.
5. Do one of the following:
   - If you want to delete the data from the portable profile after import, check **Delete original data once merged**.
   - If you do not want to delete the data from the portable profile after import, uncheck **Delete original data once merged**.

Importing logins

Identity Safe lets you import the logins that you have saved in Internet Explorer. After you set up Identity Safe vaults, the **Identity Safe Setup Successful** window appears.

You can use this window to import your logins. The imported logins appear in the **Identity Safe** menu on the **Norton Toolbar** and in the **Edit Logins** window. You can use the imported logins the same way that you use the logins that you create.

To import logins

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Identity Safe Setup** row, click **Configure**.
3. Set up Identity Safe.

4 In the **Identity Safe Setup Successful** window, do one of the following:
   - Check **Import my logins from Internet Explorer** to import all the logins that you saved in your Web browser.
   - Uncheck **Import my logins from Internet Explorer**, if you do not want to import all the logins that you saved in your Web browser.
5 In the **Identity Safe Setup Successful** window, click **Done**.

Resetting Identity Safe

There may be instances when you need to reset your Identity Safe.

You may need to reset your Identity Safe in the following occasions:

- You experience a computer failure.
- You forget your Identity Safe password.

If you forget your Identity Safe password, you cannot restore it. You can only reset your Identity Safe and store all your data again.

Norton 360 lets you enter an incorrect password three times. If your attempts are unsuccessful, Norton 360 provides you an option to reset your Identity Safe. If you reset the Identity Safe, you lose all the Identity Safe data that you stored, such as your login information, cards, and notes.

To reset your Identity Safe

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, click **Identity Protection**.
3 Under **Identity Safe**, in the **Log in to Identity Safe** row, click **Configure**.

4 In the **Enter the Password** box, type your **Identity Safe** password.
If you forget your password, Identity Safe lets you enter wrong password three times. If your attempts are unsuccessful, the **Trouble Logging In?** window appears.

5 In the **Trouble Logging In?** window, click **Reset Identity Safe**.
If you forget the Identity Safe password of your online vault, you need to provide your Norton Account credentials to reset your Identity Safe.

6 In the confirmation dialog box, click **Yes**.

Accessing Identity Safe

You can access the Identity Safe settings from the following sections of Norton 360:

- From the **Identity Safe** section in the **Identity Protection** settings window
- From the **Norton Toolbar**
- From the **Identity Protection** section in the Norton 360 main window

With Norton 360, you can access and configure some of the Identity Safe features even after the product expires. The following are the features that you can view or access after the product expires:

Edit Logins	You can view the **Edit Logins** window using the **Identity Safe** menu on the **Norton Toolbar**. Although the product is expired, you can still view all the logins that you saved for a Web site. However, you cannot save, add, or update that logins after the product expires.

Export Data	You can use this feature to take a backup of your Identity Safe data. The data that you back up are stored as .DAT file.

You must be logged in to Identity Safe to access the Identity Safe features. The Identity Safe features are supported only in the Internet Explorer, Firefox, or Chrome Web browsers.

To access Identity Safe settings from the main window

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, for the Identity Safe feature that you want to open, click **Configure**.

To access Identity Safe settings from the Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Identity Protection**.
3. Under **Identity Safe**, for the Identity Safe feature that you want to open, click **Configure**.

To access Identity Safe settings from the Norton Toolbar

1. Start your Web browser.
2. On the **Norton Toolbar**, in the **Norton** menu, click **Settings**.
3. For the Identity Safe feature that you want to open, click **Configure**.

Logging in to and logging out of Identity Safe

You can log in to or log out of Identity Safe from the following areas of Norton 360:

- The **Identity Safe** section in the **Settings** window for Identity Protection

- The **Identity** section in the Norton 360 main window
- The Norton Toolbar

To secure your Identity Safe data from others, log out of Identity Safe whenever you are away from your computer.

Identity Safe automatically logs you out of the current vault, when you are logged in to your local vault or online vault and click **Identity Safe Setup** to create a new vault

To view or edit your confidential data, you must be logged in to Identity Safe.

To log in to Identity Safe

1. In the Norton 360 main window, click **Identity**, and then click **Log in to Identity Safe**.
2. In the **Log in to Identity Safe** window, in the **Enter the Password** box, type the password of the vault you want to log in.
3. Click **Log In**.

To log out of Identity Safe

- In the Norton 360 main window, click **Identity**, and then click **Log out of Identity Safe**. You can also log out from the **Settings** window for Identity Protection.

To log in to Identity Safe from the Norton Toolbar

1. Start your Web browser.
2. On the **Norton Toolbar**, click **Identity Safe**.
3. Under **Identity Safe** menu, click **Log in to Identity Safe**.
4. In the **Log in to Identity Safe** window, in the **Enter the Password** box, type the password of the vault you want to log in.
5. Click **Log In**.

To log out of Identity Safe from the Norton Toolbar

1. Start your Web browser.

2 On the **Norton Toolbar**, click **Identity Safe**, and then click **Log out of Identity Safe**.

Configuring Identity Safe settings

You can use the various features in Identity Safe to manage your personal sensitive information. The logins, cards, and notes help you store and use your information in a secure way.

To configure Identity Safe settings

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.

2 Under **Identity Safe**, identify the feature that you want to use, and click **Configure**. Your options are:

Identity Safe Setup	Lets you set up Identity Safe vault. You can create a local vault or an online vault and store your Identity Safe data. You must log in to your Norton Account to create an online vault.

Browsing Options	Lets you configure the way you want Identity Safe to collect, store, and display the login information for the Web pages you visit. You can configure Identity Safe to display your cards that you created for the Web sites that have forms. You can also configure the autofill settings for the Web sites that contain security threats. In addition, you can do the following activities: ▪ Configure the region for your card information. ▪ Specify how you want Norton Identity Safe to use the autofill feature. ▪ Set the options that make Identity Safe to display a message to notify you that you have inserted an external drive. ▪ Set the options that make Identity Safe to warn you about the unsafe removal of external drives. ▪ Turn off the browser's password manager
Password & Security	Lets you change the password settings and the security level of your Identity Safe password. You should change your Identity Safe password frequently to keep your Identity Safe data from being misused.

Edit Cards	Lets you manage your personal information such as name, date of birth, email address, and credit card information in one place. You can use the information that you store to automatically fill forms. This feature lets you provide sensitive information without typing it when you are online. In this way, Identity Safe protects you from keyloggers that steal and misuse your identity.
Edit Logins	Lets you manage your various login information. Logins include information such as your email login credentials and Internet banking credentials. When you save all of your login information in the Identity Safe, you can do the following: ▪ Easily track all your logins ▪ Quickly launch your login Web sites ▪ View or update your password for the Web site ▪ Use folders to organize your logins ▪ Change your login settings

Edit Notes	Lets you store and manage sensitive information. You can save social security number, driver's license number, insurance policy number, and passport number. You can also save private accounts, lock combinations, documents, notes, frequent flier numbers, bank account number, security challenge questions, and legal and financial information.
Export Data	Lets you back up the Identity Safe data in .DAT or .CSV file formats. You should back up all of your Identity Safe data periodically.
Import Data	Lets you import the Identity Safe data from the backed up file or from the portable profile that you have from the older versions of Norton 360. When you import the Identity Safe data you have the following options: ▪ Merge the imported data in to the vault that you are currently logged in. ▪ Replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

Move Data Online	Lets you move your Identity Safe data that you stored in your local vault to online vault. When you move your Identity Safe data from local vault to online vault, the data in the local vault is permanently removed.
Delete Data	Lets you permanently remove the Identity Safe vault.

About Edit logins

The Edit Logins feature in Identity Safe lets you view all the logins that you want Identity Safe to manage. Login information includes information such as your email login credentials and Internet banking credentials.

Identity Safe provides you the option to save your logins when you enter your login information in a Web site's login page. You can instantly save your login information in Identity Safe.

To manage your logins, you must be logged in to Identity Safe.

Identity Safe offers the following features:

- Safely stores Web site login information
- Lets you save multiple IDs or accounts and passwords for a Web site
- Lets you organize your logins under various folders
- Intelligently searches for a particular login
- Lets you save the Web site name with a name other than the default name
- Displays the login ID and lets you show or hide the password
- Displays the strength of the password for your login

- Lets you quickly launch the Web site login page
- Fills in your login automatically when you revisit Web pages
- Lets you manually add logins
- Lets you change the URL of your saved logins
- Lets you view the last time you made changes to the settings of your saved logins
- Lets you view and fill the login details that you saved for a Web site even after Norton 360 expires. To do so, use the **Identity Safe** menu on the **Norton Toolbar** in the Web browser.

The Identity Safe features are supported in the Internet Explorer, Firefox, or Chrome Web browsers.

Norton 360 supports Google Chrome version 10.0 or later.

Saving logins

Logins are saved when you enter them for the first time. You can save multiple logins for the same Web page. You can also save the same login for different Web pages.

When you provide your login credentials on a Web site, Identity Safe displays **Save your login for this site?** on the **Norton Toolbar**. You can provide a name for your login and select the folder in which you want to save your login. The folders that you create appear in the **Folder** drop-down list in the **Save login for site** dialog box.

After Identity Safe saves a login, it automatically fills the login details next time you visit the Web site.

You must be logged in to Identity Safe to save and use autofill passwords. If the password or user name field is blank, Identity Safe does not prompt you to save the login.

Identity Safe lets you view and fill the login information that you saved for a Web site even after the product

expires. You can use the **Identity Safe** menu on the **Norton Toolbar** to view the logins.

You can only view your saved logins after Norton 360 expires, you cannot save or add any new logins.

When you try to save a login after the product expires, a pop-up window appears and suggests you to renew the subscription of the product. You can use the pop-up to renew the subscription.

To save a login

1. Go to the Web site for which you want to save your login.
2. Type your login details, and then click the option or link that logs you in.
3. On the **Norton Toolbar**, in the **Save your login for this site?** row, do one of the following:
   - If you want to save your login, click **Save**. In the **Save Login for Site** dialog box, type a name for your login in the **Name** box, select the folder in which you want to save your login from the **Folder** drop-down list, and then click **Save**.
   - If you do not want to save your login this time, click **Don't Save**.
   - If you never want to save your login, click **Never**.

To save additional logins for a Web site

1. Go to the Web page for which you want to save another login.
   Your login credentials automatically appear on the Web page.
2. Clear the login credentials that appear on the Web page.
3. Type the new login, and then click the option or link that logs you in.
4. On the **Norton Toolbar**, in the **Save your login for this site?** row, click **Save**.

5 In the **Save Login for Site** dialog box, type a name for your login in the **Name** box, select the folder in which you want to save your login from the **Folder** drop-down list.

6 Click **Save**.

Editing logins

Edit Logins lets you view all of the logins that you want Identity Safe to manage.

Edit Logins provides the following features:

- Lets you safely store Web site login information.
- Lets you save multiple IDs or accounts and passwords for a Web site.
- Lets you organize your logins under various folders.
- Intelligently searches for a particular login.
- Lets you save the Web site name with a name other than the default name.
- Displays the login ID and lets you show or hide the password.
- Displays the strength of the password for each of the logins.
- Lets you quickly launch the Web site login page.
- Fills in your login automatically when you revisit Web pages.
- Lets you manually add logins.
- Lets you change the URL of your saved logins.
- Lets you view the last time you made changes to the settings of your saved logins.

Edit Logins also lets you view and fill the login details that you saved for a Web site even after Norton 360 expires. To do so, use the Identity Safe menu on the **Norton Toolbar**.

To create a new folder

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.

2 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3 In the **Edit Logins** window, click **Create New Folder**.
4 In the **New Folder** dialog box, in the **Enter new folder name** box, type a folder name.
5 Click **OK**.
6 Click **Close**.

To add a login manually

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3 In the **Edit Logins** window, click **Create New Login**.
4 In the **New Login** dialog box, type the URL of the Web site or a name for which you want to use this login.
If it is a URL, ensure that you prefix it with HTTP.
5 Click **OK**.
6 In the **Username** dialog box, in the **Enter new username** box, type the user name of the login, and then, click **OK**.
7 In the **Information** dialog box, click **OK**.
The **Information** dialog box prompts you to set a password for the login that you created.
8 In the **Edit logins** window, in the **Password** box, type the password of your login.
9 Click **Close**.
10 In the **Save** dialog box, click **Yes** to save the changes.
The **Save** dialog box appears only if you set a password for the login that you created.

To set a password for the login that you added manually

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.

3 In the **Edit Logins** window, under **Logins**, select the login for which you want to set a password.
4 Under **Details**, next to **Password** box, click **Show**. The **Validate Password for Identity Safe** window appears. This window appears only if you have changed the Identity Safe password security level to **Ask for my password before filling out a login or form** in the **Password & Security** window.
5 In the **Validate Password for Identity Safe** window, do the following:
   - In the **Enter the Password** box, type your Identity Safe password.
   - Click **Validate**.
6 In the **Edit Logins** window, in the **Password** box, type your Identity Safe password.
7 Click **Close**.
8 In the confirmation dialog box, click **Yes** to save the changes.

To delete a login or a folder

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2 Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3 In the **Edit Logins** window, under **Logins**, select the Web site name or the folder that you want to delete.
4 Click **Delete**.
5 In the Warning dialog box, click **Yes**.
6 Click **Close**.

Managing your URL details

Edit Logins lets you view the URL of the logins that you saved. You can view the URL of the Web site logins that you save in Edit Logins.

When you save a login, you can do the following:

- Quickly launch the Web site login page using the URL

- Change the URL of the login manually
  Ensure that the URL you change belongs to the same domain as the current URL.
- View the details of the date and time when you last made to the Edit Logins settings

To quick-launch a login Web page

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3. In the **Edit Logins** window, under **Logins**, select the login for which you want to launch the Web site.
   If you have saved your login in a folder, double-click the folder and select the login.
4. Under **Details**, click the URL that is available next to the **Address** option to launch the Web site.
5. Click **Close**.

To change the URL of your login

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3. In the **Edit Logins** window, under **Logins**, select the login for which you want to launch the Web site.
4. Under **Details**, click **Change** that is available next to the **Address** option.
5. In the **Update URL** window, in the **Enter the new URL here** box, type the new URL.
   Ensure that the URL you modify is valid and is prefixed with HTTP.
6. Click **OK**.
7. In the **Edit Logins** window, click **Close**.

Changing the user name and password

Identity Safe lets you change the user name and password for the logins that you have saved in the **Edit**

Logins window. The updated information is automatically filled the next time you visit that Web page.

To change the user name

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3. In the **Edit Logins** window, under **Logins**, select the Web site name for which you want to change the user name.
4. Under **Details**, next to **Username** box, click **Change**.
5. In the **Username** dialog box, in the **Enter new username** box, type the new user name.
6. Click **OK**.
7. In the **Edit Logins** window, click **Close**.

To change the password

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Logins** row, click **Configure**.
3. In the **Edit Logins** window, under **Logins**, select the Web site name for which you want to change the password.
4. Under **Details**, next to the **Password** box, click **Show**.
   The **Validate Password for Identity Safe** window appears. This window appears only if you have changed the security level of the Identity Safe password to **Ask for my password before filling out a login or form** in the **Password & Security** window.
5. In the **Validate Password for Identity Safe** window do the following:
   - In the **Enter the Password** box, type your Identity Safe password.
   - Click **Validate**.

6 In the **Edit Logins** window, in the **Password** box, type the new password.
7 Click **Close**.
8 In the confirmation dialog box, click **Yes** to save the changes.

Updating the password for a login

Good security practice requires that you regularly change the password for a login. You can keep your login credentials in Identity Safe updated every time you change your password for a Web page. The updated information is automatically filled the next time you visit that login's associated Web page.

You can also update your new login information in Identity Safe when you are on the Web page. Identity Safe asks you if you want to update your logins.

To update the password for a login

1 Go to the Web page for which you want to change the password information.
2 Clear the password entry that Identity Safe autofilled.
3 Type the new password, and then click the button or link that logs you in.
4 In the **Save new password for login?** menu bar, click **Save**.

About Edit Cards

The **Edit Cards** option in Identity Safe lets you manage your personal information such as name, date of birth, email address, and credit card information in one place.

You can use the information that you store in the cards to do the following:

- Automatically fill forms
- Provide sensitive information without having to type it while you are online

In this way, Identity Safe protects you from keyloggers that steal and misuse your identity.

Some Web sites have forms with fields for credit cards or other personal information. The **Identity Safe** menu on the **Norton Toolbar** lists the cards that you created for autofill. You can choose a card from the list to fill the forms automatically.

You can add, view, edit, and duplicate the details of any card that you create. You can also delete a card if it is no longer needed.

In addition, Edit Cards provides you the following features:

- Lets you password-protect the card to protect yourself from misuse of your sensitive information and personal information
- Recognizes the Web pages that have forms and immediately displays a pop-up window with the list of cards
- Provides you a quick view of any of your cards that is not password-protected

  Identity Safe provides additional security for your password-protected cards by not displaying the summary of the card

When you are on a Web page that has forms, the **Fill fields on this page?** menu bar in the **Norton Toolbar** displays the cards that you saved. You can click the **Fill Form** option in the **Fill fields on this page?** menu bar and select the card that you want to use to fill the Web site. You can also use the **Fill with Identity Card** option in **Identity Safe** menu to select the cards.

Adding cards

The cards in the **Edit Identity Cards** window help you to automatically fill forms on Web sites with a single click. You can create cards to store information, such as personal details, contact details, and credit card details. You can provide a card name to help you identify a specific card.

If you have more than one credit card, you can create multiple cards with different sets of information. When you visit a transactional Web site, you can provide the credit card details that are present in any of the cards that you created.

You can also create anonymous cards for use on unfamiliar Web sites where you may be uncomfortable providing your personal information. You can automatically fill online forms when you visit a Web site.

To add a card

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Cards** row, click **Configure**.
3. In the **Edit Identity Cards** window, click **Add Card**.

4 Use the following tabs to type your card details:

General	Provide details such as card name, name, gender, and date of birth. You can set a password and provide additional security for your card. Online form filling is language-specific. In the **Country/Region** box, the country United States is selected by default. You should change your region and create a new card before you fill online forms for any other language.
Contact	Provide your contact information in this section. Contact information includes your email address, postal address, and phone numbers.
Credit Card	Provide your credit card details such as the type of the card, expiration date, and card number in this section. You cannot enter a credit card number of more than 16 digits.

5 Click **Save**.

6 Click **Close**.

Editing, deleting, or duplicating cards

All the cards that you have saved in Identity Safe are listed in the **Edit Identity Cards** window. You can select, view, duplicate, and edit the details of any card that you created. You can delete a card if it is no longer needed. You can also duplicate a saved card and change only the fields that you want to change.

You can view a summary of the card that you created. You can select any of the cards that are present in the list of cards at the left pane of the **Edit Identity Cards** window. When you select a card, you can view a summary of the card.

When you lock your card with a password, Identity Safe provides additional security to your card. You cannot view the summary of the locked card. You cannot edit, delete, or duplicate a card unless you provide the password.

If you have multiple cards, use the scroll arrows to browse the list.

When you create, duplicate, or edit a card, the card's region is set to the user's default region. If you browse to a Web site other than the default region and use the card to fill the form on that Web site, the fields may not fill correctly. For example, your card has a default United States region but you are on a France Web page. In this case, you must use the card with France as the region to fill the Web page form.

To edit a card

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Cards** row, click **Configure**.
3. In the **Edit Identity Cards** window, select the card that you want to edit.
4. Click **Edit Card**.
5. Modify the required details that you want to change.
6. Click **Save**.
7. Click **Close**.

To delete a card

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Cards** row, click **Configure**.

3 In the **Edit Identity Cards** window, select the card that you want to delete.
4 Click **Delete Card**.
5 In the Warning dialog box, click **Yes**.
6 Click **Close**.

To duplicate a card

1 In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2 Under **Identity Safe**, in the **Edit Cards** row, click **Configure**.
3 In the **Edit Identity Cards** window, select the card that you want to duplicate.
4 Click **Duplicate Card**.
5 Modify the details that you want to change.
6 Click **Save**.
7 Click **Close**.

About Edit Notes

Identity Safe stores and manages your sensitive information. It becomes difficult to manage all of the identity numbers that you use when you browse the Web. The **Edit Notes** option in Identity Safe stores all your sensitive IDs in a very secure way and lets you use them easily when you are online. You can use Edit Notes to save information such as social security number, driver's license number, insurance policy number, and legal and financial information.

Editing Notes

You can use the **Edit Notes** option in Identity Safe to store your personal information, which you can retrieve and use when needed. You can use this information to fill out Web site registration forms. You can also view, edit, and delete the notes that you have saved.

To create Notes

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
3. In the **Edit Notes** window, under **Details**, in the **Title** box, type a title for the note you want to save.
   If a note already exists, click **Create New Notes**, and then under **Details**, in the **Title** box, type a title for the note you want to save.
4. Type any additional information in the **Information** box.
5. Click **Save**.
6. In the **Edit Notes** window, click **OK**.

To edit Notes

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
3. In the **Edit Notes** window, under **Title**, select the title of the note that you want to edit.
4. Click **Edit Notes**, and modify the information under **Details**.
   You can change the category, modify the title, and edit the additional information that you have provided.
5. Click **Save**.
6. In the **Edit Notes** window, click **OK**.

To delete Notes

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Edit Notes** row, click **Configure**.
3. In the **Edit Notes** window, under **Title**, select the title of the note that you want to delete.
4. Click **Delete Notes**.

5 In the Warning dialog box, click **Yes**.
6 In the **Edit Notes** window, click **OK**.

About exporting and importing Identity Safe data

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer. The backup files are saved as .DAT files.

You can protect the files that you backed up with a password. Symantec recommends that you use a password to keep your Identity Safe data more secure. The backup password does not need to be the same as your Identity Safe password. You must provide the password when you restore the Identity Safe data that you backed up.

You can import your Identity Safe data from the file that you previously backed up. You can also import the Identity Safe data from the portable profile.

When you import the Identity Safe data you have the following options:

- Merge the imported data in to the vault that you are currently logged in.
- Replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

You can also delete the data once the import is complete.

Exporting your Identity Safe data

You can export your Identity Safe data for security purposes, data recovery, or when you transfer your Identity Safe data to a new computer.

You can retrieve Identity Safe data when your product expires.

To export your Identity Safe data

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Export Data** row, click **Configure**.
3. In the **Export Identity Safe Data** window, select the **File Format**.
   You can select one of the following:
   - Identity Safe Backup Format
   - Plain text
4. In the **Export my data to** box, type or browse to the location to which you want your data saved.
5. Type the name that you want to assign to the file.
6. If you want to back up your data with a password for more security, type and confirm the password.
7. Click **OK**.
8. In the confirmation dialog box, click **OK**.

Importing your Identity Safe data

You can import your Identity Safe data from the file that you previously backed up. You can also import the Identity Safe data from the portable profile that you saved in the older version of Norton 360.

You can merge the imported data in to the vault that you are currently logged in or replace the existing Identity Safe data that you stored in your vault that you are logged in with the imported data.

The **Merge with existing data** and **Replace existing data** options appear only when you import Identity Safe data from a backup file.

When you import Identity Safe data from local or portable profile, you can only merge the data. The **Delete Original data once merged** option appears when you import the data from local or portable profile. By default, this option is enabled.

To restore your data

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Import Data** row, click **Configure**.
3. In the **Import Identity Safe Data** window, under **Import my data from**, select one of the following options:
   - **Portable Profile (Drive: Drive:\)**

     This option appears only if you connect an external drive with a portable profile.
   - **Local Profile**

     Select this option if you want to import the Identity Safe data from your local vault to online vault. This option appears only if you are logged in to your online vault.
   - **Backup File**

     If you select this option, you must type or browse to the location of the file from which you want to import the data.
4. If you backed up your data with a password, in the **Password** box, type the password.
5. If you want to import the data from a backup file, under **While importing data**, select one of the following options:
   - **Merge with existing data**
   - **Replace existing data**
6. Click **OK**.
7. In the confirmation dialog box, click **OK**.

About Browsing Options

Browsing Options lets you configure the way you want Identity Safe to collect, store, and display the login information for the Web pages you visit. You can configure Identity Safe to display your cards that you created for the Web sites that have forms. You can also

configure the autofill settings for the Web sites that contain security threats.

You can configure the following options in the **Browsing Options** window:

Offer to save my credentials when I log in to web sites	Prompts you to save the login credentials for the Web sites that you visit.
Display my Logins each time I visit a page with multiple Logins	Configures Identity Safe to display your logins each time you visit a Web site that has multiple logins.
Autofill my logins when I visit websites	Autofills your login details when you visit a Web site.
Display my Identity Cards each time I visit a page with fillable form	Displays your Identity Cards each time you visit a Web page with forms to fill your personal details.

In addition, you can use the **Autofill sites containing security threats** option to specify how you want Identity Safe to respond to the Web sites that have security threats. You can also turn off the browser's password manager using the **Turn off the browser's password manager** option.

About Password & Security

You can use Password & Security to change your Identity Safe password. You can also use this option to set the level of security that you want for Identity Safe password usage.

The following sections let you change the Identity Safe password and set security levels for your password:

Identity Safe Password	Change your Identity Safe password and set a new password hint using the **Change Password** option.

Password Security	

	Specify the Identity Safe password security level. Identity Safe provides four levels of security to protect your Identity Safe password. Choose one of the following options: ▪ **Ask for my password at the beginning of each login session** Prompts for your Identity Safe password the first time you access Identity Safe. If you are logged in to Windows, you do not need to provide the password again. You should use this option to make your login credentials more secure. ▪ **Ask for my password before filling out a login or form** Prompts for your Identity Safe password with every online form before it autofills any login. You can specify that individual logins require your Identity Safe password before autofill occurs. ▪ **Automatically log out of Identity Safe if computer is inactive for** Automatically logs you out of Identity Safe when your computer is idle for the time that you specify.

	You can select 15, 30, or 45 minutes. Use this option if other people have access to your computer. **No password needed. Automatically log me in when Windows is started** Set this option if you want to automatically log in to Identity Safe when Windows is launched. Symantec recommends that you do not choose this option. Setting this option is specific to Windows user account. **Ask for my password upon resuming from suspend** Prompts you for your Identity Safe password when your system restores from suspended state. This option prevents misuse of your Identity Safe data by validating your Identity Safe password each time your system restores from suspended state. Norton 360 prompts you to enter your Identity Safe password only if you had logged into your Identity Safe vault when the system moved to the suspended state.

	You must validate your Identity Safe password each time you change the security level of the vault to a setting that is less secure than the current security level.

Changing the Identity Safe password

You should change your Identity Safe Password regularly to prevent unauthorized access to your personal information in Identity Safe. You can change the password by using the **Password & Security** option in **Settings** window.

If you want to change the Identity Safe password of your online vault, the password you provide must have the following characteristics:

- At least eight characters
- At least one capital letter
- At least two numerals (0 through 9)
- At least one symbol (for example, * > & $ %)
- The password must not match with your Norton Account user name or password.

You can set your password hint here if you did not provide it when you configured Identity Safe.

To change the Identity Safe password

1. In the Norton 360 main window, click **Identity**, and then click **Manage Identity Protection**.
2. Under **Identity Safe**, in the **Password & Security** row, click **Configure**.
3. In the **Password & Security** window, click **Change Password**.
4. In the **Change Identity Safe Password** window, type the current password and the new password, and confirm the new password.
5. Click **OK**.

6 In the confirmation dialog box, click **OK**.

About Norton Toolbar

When you install Norton 360, it adds **Norton Toolbar** to Internet Explorer, Firefox, and Chrome Web browsers.

You have the following options in the **Norton Toolbar**:

Norton menu	Lets you access Identity Protection and other settings. The following options are available in the **Norton** menu: ▪ **Report Site** ▪ **Minimize Toolbar** ▪ **Settings** ▪ **Community Buzz** ▪ **Go to Norton Safe Web website** ▪ **Enable Norton Safe Web** ▪ **Enable Norton Safe Search/Disable Norton Safe Search** ▪ **My Norton Account** ▪ **Launch Tutorial** ▪ **Help** The **Minimize Toolbar** option appears only in the Internet Explorer browser. Also, the **Community Buzz** option is available only in English-language versions of Windows.

Norton Safe Search	Lets you perform an enhanced Internet search using Norton Safe Search. You can type a search string in the **Norton Safe Search** box and perform a search. When you search using the search box, a pop-up window appears and displays the relevant search results. Norton 360 uses the Ask.com to display the search results. By default, the **Norton Safe Search** box is hidden. After you install Norton 360 and connect to Internet, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search.
Safe Web indicator	Lets you know if the Web site you visit is safe or unsafe. The Antiphishing and Norton Safe Web options under the **Safe Surfing** section on the **Settings** window of the **Identity Protection** option in the main **Settings** window, analyze the security level of the Web sites you visit. It then displays the results in the **Norton Site Safety** pop-up window.

Identity Safe menu	Lets you view the logins and cards that you have saved in Identity Safe. Some Web sites have forms to fill or require login information. You can use the **Identity Safe** menu to fill the details in those Web sites. The **Identity Safe** menu displays the list of all logins and cards that you saved. You can select a login from the list and a use it to log in to the Web site. You can also select a card from the list and use to fill forms. You can use the **Option** submenu to manage your logins, cards, and notes and to access the **Identity Protection** settings window. In addition, you can edit and delete a login using the Identity Safe menu. You should be logged in to any of the Identity Safe vault to access the **Identity Safe** menu.

In Google Chrome Web browser, the **Norton Toolbar** can be accessed as a Chrome Extension. In the Extensions page of the Chrome browser, you can enable or disable the **Norton Toolbar**, and uninstall the **Norton Toolbar** from your Chrome browser.

If the **Norton Toolbar** is enabled, you can access the following options:

Allow in incognito	Lets you browse internet in stealth mode without storing data of your browsing session in browsing or download histories.

Allow access to file URLs	Lets you view the URL location of the downloaded file.

If you have uninstalled the **Norton Toolbar** from your Chrome browser, you must reinstall Norton 360 to access the **Norton Toolbar** on your Chrome browser again.

Norton 360 lets you install the **Norton Toolbar** for free even after you uninstall the product. When you uninstall Norton 360, it offers to leave the **Norton Toolbar** without any cost to search and browse safely over the Internet. However, when you choose to install the **Norton Toolbar**, the only features that you have are Norton Safe Search and Norton Safe Web.

Your computer must be connected to the Internet to avail this option. Norton 360 does not offer to leave the **Norton Toolbar** if you upgrade your product to the latest version or choose to reinstall another Norton product.

Hiding and showing the Norton Toolbar

You can hide the **Norton Toolbar** if you do not want to see the evaluation of every Web site that you visit. When you hide the toolbar, Norton 360 does not display the **Norton Site Safety** pop-up window. However, Norton 360 notifies you about suspicious and fraudulent Web sites or if an error needs your attention.

To hide or show the Norton Toolbar in the Internet Explorer and FireFox Web browsers

1. At the top of your browser window, click **View**.
2. On the **Toolbars** submenu, do one of the following:
   - Uncheck **Norton Toolbar** to hide the toolbar.
   - Check **Norton Toolbar** to show the toolbar.

To hide or show the Norton Toolbar in the Chrome Web browser

1. At the top-right corner of your Web browser, click the **Wrench** icon.
2. In the main menu that appears, click **Tools > Extensions**.
3. In the Web page that appears, under Extensions, do one of the following:
   - Click **Disable** to hide the toolbar.

     

     You can also hide the **Norton Toolbar** by right-clicking the **Norton Toolbar** icon near the **Wrench** icon. However, you cannot enable the **Norton Toolbar** using the **Norton Toolbar** icon.
   - Click **Enable** to show the toolbar.

To hide the Norton Toolbar button in the Chrome Web browser

- At the top-right corner of your Web browser, right-click the **Norton Toolbar** icon, and then click **Hide** option.

To show the Norton Toolbar button in the Chrome Web browser

1. At the top-right corner of your Web browser, click the **Wrench** icon.
2. In the main menu that appears, click **Tools > Extensions**.
3. Under **Extensions** page, click **Show** option.

Accessing Identity Safe settings from the Norton Toolbar

When you install Norton 360, it adds the **Norton Toolbar** to the Internet Explorer, Firefox, and Chrome Web browsers. The **Identity Safe** menu on the **Norton Toolbar** provides quick links to access the options under Identity Safe.

To access the Identity Safe settings from the Norton menu

1 Start your Web browser.

2 On the **Norton Toolbar**, in the **Norton** menu, select one of the following:

Report Site	Lets you report to Symantec about the current Antiphishing evaluation.
Minimize Toolbar	Lets you minimize the Norton Toolbar. When you check this option, the **Identity Safe** phrase and the Safe Web phrase disappear and only the **Identity Safe** and Safe Web indicators remain. In addition, the size of the **Norton Safe Search** box is reduced. The **Minimize Toolbar** option appears only in the Internet Explorer browser.
Settings	Lets you open the**Identity Protection** settings window and configure the Identity Safe options.

Community Buzz	Lets you view the community site rating of the Web sites you visit. You can click **Community Buzz** to know further details about the Web sites. Norton Safe Web rates the sites and provides detailed reports. In addition, you can see user reviews and post your reviews about the Web sites. When you have not opened any Web site, you can click **Community Buzz** to visit the Norton Safe Web site. You can provide the address of any Web site and find the security details, Norton rating, and community reviews of the Web site. The **Community Buzz** option is available only in English-language versions of Windows.
Go to Norton Safe Web website	Lets you open the Norton Safe Web site http://www.safeweb.norton.com.
Enable Norton Safe Web	Lets you turn on the Norton Safe Web feature which provides a safe online browsing experience. The following are the unique features of Norton Safe Web: ▪ Displays the site safety rating icons next to the search results ▪ Displays the site safety rating icons when you are on a Web site

Enable Norton Safe Search/ Disable Norton Safe Search	Lets you view the **Norton Safe Search** box. You can type a search string in the Norton Safe Search box and perform a search. The search box displays relevant search suggestions in a pop-up window. By default, the **Norton Safe Search** box is hidden. After you install Norton 360 and open Internet Explorer, Firefox or Chrome browser, an alert message is displayed. The alert message prompts you to enable Norton Safe Search. You can choose to enable or disable Norton Safe Search. If you want to disable Norton Safe Search, you can use the **Disable Norton Safe Search** option.
My Norton Account	Lets you open the Web site https://account.norton.com. Norton Account lets you register your product with Symantec and manage all of your Norton products in one place.
Launch Tutorial	Lets you view the online tutorial to learn more about Identity Safe.
Help	Lets you view the **Norton** menu help page.

Accessing the Identity Safe menu

The Identity Safe menu on the **Norton Toolbar** lets you view and manage the logins, Identity cards, and notes that you saved.

You can also access the **Identity Protection** of the **Settings** window using the **Identity Safe** menu

In addition, you can do the following:

- Navigate to any Web site for which you have saved the login credentials.
- Submit feedback about your experience with Identity Safe.
- Export your Identity Safe data.
- Import your Identity Safe data from the file you backed up or from the portable profile.
- Convert your local vault to online vault.

When you visit any login Web page without setting up your Identity Safe, a menu bar appears in the **Norton Toolbar**. You can use the **Setup** option that is available in the menu bar to set up Identity Safe.

Identity Safe menu lets you view the logins that you saved even after the product expires. You can use this option to autofill the login details of the saved login. As Antiphishing is disabled when the product is expired, it is not recommended to autofill the login details. In addition, you can view the **Identity Protection** settings window. However, you cannot view, access, or configure all the features in the Identity Protection settings after Norton 360 expires.

To access your logins from the Identity Safe menu

1 Start your Web browser.

2 On the **Norton Toolbar**, in the **Identity Safe** menu, select one of the following:

Merge Portable Data (Drive:\)	Lets you merge the Identity Safe data from your portable profile that you have created from the previous versions of Norton 360. This option appears in the **Identity Safe** menu only if you have connected an external drive with portable profile.
Stop ignoring this page	You can select this option if you want to autofill the login information in the current Web page. This option appears in the **Identity Safe** menu only if you select **Ignore this page** option under **Options**.
Recently Used Logins	Lets you view the list of logins that you used recently in that computer. You can view only the latest five logins that you used.
All Logins	Lets you view the list of all the logins you have stored in Identity Safe.

Options

Lets you view the various options that are available in Identity Safe.

The options are:

- **Edit Logins**

  Lets you open the **Edit Logins** window.
- **Edit Identity Cards**

  Lets you open the **Edit Identity Cards** window.
- **Edit Notes**

  Lets you open the **Edit Notes** window.
- **Settings**

  Lets you open **Identity Protection** of the **Settings** window.
- **Export**

  Lets you open the **Export Identity Safe Data** window.
- **Import**

  Lets you open the **Import Identity Safe Data** window.
- **Move to Online**

  Lets you open the **Move Identity Safe Data Online** window.

  You can move your Identity Safe data that you stored in your local vault to online vault. You must log in to your Norton Account to move your data online.

  This option appears in the **Identity Safe** menu only when you are logged

	in to your local vault. ▪ **Ignore this page** You can select this option if you do not want to autofill the login information in the current Web page.
Report Issue	Lets you open the Norton Feedback Web site. You can submit feedback on your experience with Identity Safe. You can also submit the problems that you encountered with Identity Safe. You can select from the list of problems or you can describe your problem.
Fill Login Fields	Lets you view the login information that you have saved for that Web site.
Fill with Identity Card	Lets you use a card while you are on a Web page that has forms. The option displays the cards that you saved from which you can choose the one you want to use to fill the form. The option appears only when you are on a Web site that has forms.

Log in to Identity Safe/Log out of Identity Safe	Lets you log out of or log in to Identity Safe. You should log out of Identity Safe to secure your Identity Safe data when you are away from your computer.

Protecting your home network

10

This chapter includes the following topics:

- About the Network Security Map

About the Network Security Map

A home network typically consists of the computers and other devices that share your Internet connection. The Network Security Map helps you view and manage your network.

After you configure Network Security Map, Norton 360 automatically detects the devices that are connected to your network and lists them in the Network Security Map. You can view devices and customize the Network Security Map to remotely monitor the computers on which a Norton product is installed.

Ensure that the computers that you want to remotely monitor have a version of a Norton product that supports Remote Monitoring.

You can access the Network Security Map from the **My Network** settings window.

You can monitor the following items in the Network Security Map:

- Security status of the computers that are connected to the network
- Status of the protection features of the computers that are connected to the network

- Subscription status and Norton product version of the computers that are connected to your network
- Status of your wireless network connection
- Connection status of the devices that are on the network
- The known, unknown, or intruder devices that are on your network

You can grant or deny permission to the networked devices to access your computer.

You can also modify details about a computer or device that is connected to your network.

Viewing devices on the Network Security Map

The **Network Security Map** window provides a pictorial representation of the devices on the network to which your computer is connected. You can view the details of each device, such as device name, security status, and IP address.

The **Network Security Map** window also provides the security status of the following computers:

- The computer on which you view the remote monitoring status (MY PC)
- The computers that are remotely monitored

The trust level of the device appears at the bottom of the icon in the network map.

Norton 360 displays devices in the following order:

- MY PC
- Devices with online connection status
- Devices with offline connection status

When you connect a new device to your network, Norton 360 automatically refreshes the **Network Security Map** window and displays the device.

Norton 360 requires you to configure the Symantec Security Driver to open the Network Security Map. You cannot install the Symantec Security Driver when you run LiveUpdate. You can either allow the Norton LiveUpdate to complete or close the Norton LiveUpdate session before you install the Symantec Security Driver.

To view devices on the Network Security Map

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. If the **Product Configuration** panel appears, click **Continue**.
   The **Product Configuration** panel appears when you click **Network Security Map** for the first time. The **Product Configuration** panel helps you install Symantec Security Driver that is required to view the **Network Security Map** window. The process of installation of the Symantec Security Driver disrupts your network connection temporarily.
4. Under **Network Security Map**, click **Configure**.
   The **Network Security Overview** window lets you view the summary of features of the Network Security Map. The **Network Security Overview** window appears in the following instances:
   - When you open the **Network Security Map** window for the first time.
   - When you turn on **Welcome Screen at Startup** in the **Settings** window.
5. If the **Network Security Overview** window appears, click **OK**.
   If you do not want to view the **Network Security Overview** window in the future, check **Do not show this again** before you click **OK**.
6. In the **Network Details** drop-down list, select the network that lists the device for which you want to see the details.

To view the details of a device on the Network Security Map

❖ In the **Network Security Map** window, click a device icon.
You can use the scroll arrows to view the devices that are listed in the network map.
The device details section that is located below the network map displays the following details:

Device Name	Shows the name of the device For a computer, the Network Security Map displays the NetBIOS name by default. However, the Network Security Map displays the name of the device as NEW if it meets the following conditions: ▪ The device does not have a NetBIOS name ▪ The device has a firewall that is enabled You can change the device name in the **Edit Device Details** window.
Adapter Manufacturer	Shows the name of the network adapter manufacturer of the device The adapter manufacturer's name is based on the physical address (also known as Media Control Access address or MAC address) of the device.

Category	Shows the category to which the device belongs The device category icon provides details on the connection status and security status. Norton 360 labels all unknown devices as NEW and sets the category as GENERIC DEVICE. This category may include computer-related devices, such as printers, media devices, and game consoles. You can change the device category in the **Edit Device Details** window.
Security Status	Shows how well your computer is protected from threats, risks, and damage The security status appears only for **MY PC** and the computers that are remotely monitored.
Remote Monitoring	Shows the connection status of Remote Monitoring The statuses are: ON OFF You can turn off Remote Monitoring for an individual computer or for all the computers that you remotely monitor.

Trust Level	Shows the access level that is granted to a remote device to connect to your computer The initial trust level is set based on the configuration of your computer. You can set trust level for all devices other than **MY PC**.
Connection	Shows the status of the connection The statuses are: **ONLINE** **OFFLINE**
Physical Address	Shows the physical address (also known as the Media Access Control address or MAC address) of the computer or device
IP Address	Shows the IP address of the computer or device If you change the IP address of a device, the updated IP address appears in the **Network Security Map** window when you refresh the list.

Turning off or turning on Network Security Overview

The **Network Security Overview** window provides a brief summary about the following features:

- Wireless Security
- Remote Monitoring
- Network Map
- Trust Controls

You can click each of the features and read the summary to learn more about using Network Security Map to manage your home network. By default, the **Network Security Overview** window appears each time you open **Network Security Map**.

If you do not want to view the **Network Security Overview** window, you can turn it off. Turning off the **Network Security Overview** window does not affect the performance or security of your computer.

You can also turn off the **Network Security Overview** window if you check **Do not show this again** option that is available at the bottom of the **Network Security Overview** window.

To turn off Network Security Overview

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. Under **Network Security Map**, in the **Welcome Screen at Startup** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**.
5. Click **Close**.

To turn on Network Security Overview

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. Under **Network Security Map**, in the **Welcome Screen at Startup** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**.
5. Click **Close**.

Setting up Remote Monitoring

You can set up Remote Monitoring by allowing computers on your network to communicate with your computer.

Ensure that the computers that you want to remotely monitor have a version of a Norton product that supports Remote Monitoring.

Norton 360 requires a Passkey to set up Remote Monitoring. You must type the same Passkey for all the computers that you want to remotely monitor.

After you set up Remote Monitoring, you can connect any computer to your network and enter the same Passkey. Norton 360 automatically identifies the computer and connects it to the Network Security Map.

To set up Remote Monitoring

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. On the left side of the **Network Security Map** window, under **Remote Monitoring**, click **Setup**.
5. In the **Remote Monitoring Setup** window, type a Passkey.
   The Passkey should be between 6 and 20 characters in length. The Passkey is case sensitive.
6. Under **Choose the default mode for Computer Discovery**, select one of the following options:

Computer Discovery always on	Lets your computer always discover other computers that are connected to the network
Computer Discovery on only when Network Security Map screen is displayed	Lets your computer discover other computers that are connected to the network when the **Network Security Map** window is open

7. Click **OK**.
8. Set up Remote Monitoring for all other computers that you want to monitor remotely.

Turning off Remote Monitoring

When you turn off Remote Monitoring, you stop remote monitoring of the computers that are connected to your network.

You can turn off Remote Monitoring for the following:

- All of the computers that you remotely monitor
- An individual computer that you remotely monitor

You can turn off Remote Monitoring only after you complete the Remote Monitoring Setup process.

To turn off Remote Monitoring for all computers

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. On the left side of the **Network Security Map** window, under **Remote Monitoring**, click **Disable**.
5. In the confirmation dialog box, click **Yes**.

To turn off Remote Monitoring for an individual computer

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. In the **Network Security Map** window, in the network map, click the computer for which you want to disable Remote Monitoring.
5. In the device details area, next to **Remote Monitoring**, click **Disable**.
6. In the confirmation dialog box, click **Yes**.

Adding a device to the Network Security Map

You can manually add a computer or device to the Network Security Map.

You can add the following details when you add a device:

- The name or description
- The IP address or physical address

The Network Security Map finds any computers that are connected to your network. However, you can add the computers and the devices that are currently not connected.

Norton 360 adds to the Trust Control network all the devices that you manually add to Network Security Map. You can select the Trust Control network in the **Network Details** drop-down list to view the devices that you added. You can also edit the name of the device.

You cannot edit the Trust Control network details.

The default trust level of the devices that you add to the Network Security Map is Protected. However, you can change the trust level of the devices.

If you trust a device that is not on your network, you can expose your computer to potential security risks.

To add a device to the Network Security Map

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. On the left side of the **Network Security Map** window, under **Total in Network**, click the plus symbol.
5. In the **Add a Device** window, in the **Name** box, type the name of the device that you want to add to the Network Security Map.
   The maximum character length of the device name is 15 characters.

6 In the **IP or Physical Address** box, type the IP address or physical address of the device that you want to add to the Network Security Map.
You can use the following formats in the **IP or Physical Address** box:

IPv4 address	172.16.0.0
IPv6 address	fe80::12ac:fe44:192a:14cc
Physical address	11-22-c3-5a-fe-a4
Resolvable host	ftp.myfiles.com

The address that you provide is not verified until the device is physically found on the network.

7 Click **Add Device**.

Finding a computer's IP address

You can find a computer's IP address in various ways. On Windows 2000/XP, Windows Vista, and Windows 7 computers, you can use Ipconfig to find the IP address of a computer.

Ipconfig reports the IP address of its local computer only. You must run this program on the computer that you want to identify.

To find an IP address by using Ipconfig on Windows 2000/XP

1 On the computer you want to identify, on the Windows taskbar, click **Start > Run**.
2 In the **Run** dialog box, type `cmd`.
3 Click **OK**.
4 At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
5 Write down the IP address.

To find an IP address by using Ipconfig on Windows Vista

1. On the computer you want to identify, on the Windows taskbar, click **Start**.
2. In the **Start Search** text box, type `cmd`, and then press **Enter** on your keyboard.
3. At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
4. Write down the IP address.

To find an IP address by using Ipconfig on Windows 7

1. On the computer you want to identify, on the Windows taskbar, click **Start**.
2. In the **Search programs and files** text box, type `cmd`, and then press **Enter** on your keyboard.
3. At the command prompt, type `ipconfig`, and then press **Enter** on your keyboard.
4. Write down the IP address.

Editing device details

You can change the name and category of a device that is available on the Network Security Map. You can select the categories such as Generic Device, Laptop, Media Device, or Game Console.

You cannot change the category of the device that you added manually. By default, Norton 360 displays the category of the manually added device as **USER DEFINED**.

The **Network Security Map** window displays different icons, depending on the category that you select. Icons help you identify the devices that are listed in the network map.

To edit the details of the device that is on your network

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.

4 In the **Network Security Map** window, in the network map, click a device icon.
5 In the device details section, next to **Device Name**, click **Edit**.
6 In the **Edit Device Details** window, in the **Name** box, type a new name.
The maximum character length of the device name is 15 characters.
7 In the **Category** drop-down list, click one of the following device categories:
- **GENERIC DEVICE**
- **DESKTOP PC**
- **LAPTOP**
- **SERVER PC**
- **NETWORK PRINTER**
- **ROUTER/SWITCH**
- **CABLE/DSL MODEM**
- **MEDIA DEVICE**
- **GAME CONSOLE**
- **PDA/MOBILE PHONE**
- **NETWORK STORAGE DEVICE**
- **WEB CAMERA**
- **TABLET**
- **MUSIC PLAYER**
- **TV**

8 Click **OK**.

To edit the name of the device that you added manually

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **My Network**.
3 In the **Network Security Map** row, click **Configure**.
4 In the **Network Security Map** window, in the **Network Details** drop-down list, click **Trust Control**.
5 In the network map, select a device that you added.

6 In the device details area, next to **Device Name**, click **Edit**.
7 In the **Edit Device Details** dialog box, in the **Name** box, type a new name.
8 Click **OK**.

Editing network details

You can view the details and change the name of your network in the **Edit Network Details** window.

You cannot edit the Trust Control network details.

To edit network details

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, under **Detailed Settings**, click **My Network**.
3 In the **Network Security Map** row, click **Configure**.
4 In the **Network Security Map** window, on the right side of **Network Details**, click **Edit**.
5 In the **Edit Network Details** dialog box, in the **Network Name** box, type a new name.
6 Click **OK**.

Changing the trust level of your network and devices

The trust level determines the default level of access that devices on your network have to your computer. Any device on your network that is not explicitly Trusted or Restricted uses the trust level of your network. The initial network trust level is set based on the configuration of your computer.

Ensure that you change the trust level of a device to Full Trust, if it is a known device, and is connected to your network.

The following conditions are necessary for the trust level of a device to be Shared:

- The computer should not have a public IP address.

Your computer does not have a public IP address if it is not directly connected to the Internet.

- The computer should be connected to a LAN through a secure connection.
- The network category should be private in Windows Vista.

In addition, the trust level of a device is Shared in any of the following cases:

- When the computer on the network has one or more folders or printers that are shared
- When the computer is Media Center compatible (for example, if you have Windows XP Media Center Edition, Windows Vista Home Premium, Windows Vista Ultimate, Windows 7 Home Premium, Windows 7 Professional, or Windows 7 Ultimate)

If you use a wireless network that is not secure, the default trust level of all the devices that are on the network is **Protected**.

The trust level of a device also depends on the trust level of its network. When you change the trust level of a network, Norton 360 assigns the same trust level to all the devices that are connected to that network. However, Norton 360 does not change the trust level of the devices that you individually trust or restrict.

You can modify these settings if you want to change the trust level for the following:

- Your network
- Devices that are connected to the Network Security Map

To change the trust level of your network

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. In the **Network Security Map** window, on the right side of **Network Details**, click **Edit**.

5 In the **Edit Network Details** window, next to **Trust Level**, click **Edit**.
You can view the details of the network in the **Edit Network Details** window before you change the trust level.

6 To select a trust level for a network, in the **Edit Network Trust Level** window, click one of the following:

FULL TRUST	Adds the network to the Trusted list All the network traffic that your computer receives from a Trusted network is filtered and allowed through firewall. However, known attacks and infections are still monitored. You should select this setting only when you are sure that the network is completely safe.
SHARED	Adds the network to the Shared list All the network traffic that your computer receives from a Shared network is filtered. Only shared resources on your computer, such as files, folders, and printers are allowed. You should select this setting if you want the firewall to protect you from all traffic except those that pertain to file and printer sharing.
PROTECTED	Adds the network to the Protected list A network is in the Protected Trust Level when it has not been classified as Trusted, Shared, or Restricted. You remain protected from known attacks and all unexpected traffic.

RESTRICTED	Adds the network to the Restricted list The devices that are on Restricted network cannot communicate with your computer. However, you can still use the network to browse Web sites, send email messages, or transmit other communications.

7 Click **OK**.

To change the trust level of a device

1 In the Norton 360 main window, click **Settings**.
2 In the **Settings** window, click **My Network**.
3 Under **Network Security Map**, in the **Trust Control** row, click **Configure**.
4 In the **Network Security Map** window, do one of the following:
   - To edit the trust level of a device that you manually added, in the network map, click the device.
   - To edit the trust level of a device that is on your network, in the **Network Details** drop-down list, click **Local Area Connection**, and then click the device.
5 In the device details section, next to **Trust Level**, click **Edit**.

6 To select a trust level for a device, in the **Edit Device Trust Level** window, click one of the following:

FULL TRUST	Adds a device to the Full Trust list Full Trust devices are monitored only for known attacks and infections. You should select this setting only when you are sure that the device is completely safe.
RESTRICTED	Adds a device to the Restricted list Restricted devices do not have access to your computer.
USE NETWORK TRUST (trust level)	Adds a device to a default trust level The devices that are removed from the Full Trust level or Restricted trust level take the default trust level of the network. The trust level of the network can be Full Trust, Restricted, Protected, or Shared.

7 Click **OK**.
Norton 360 displays the trust level status of each restricted device on the icon of the device.

Excluding a device from Intrusion Prevention scan

The Intrusion Prevention System in Norton 360 scans all the network traffic that enters and exits your computer. When a device on your network requests access your computer, Intrusion Prevention scans this request to ensure that it is not a virus attack. Scanning every request from all the devices that access your

computer increases the scan time which slows down the network speed of your computer.

If you know that a specific device on your network is safe, you can apply Full Trust level to this device. In addition, you can exclude this specific device from Intrusion Prevention scan. When you exclude a device from Intrusion Prevention scan, Norton 360 trusts this device and does not scan any information that is received from this device. This improves the network speed of your computer and helps the trusted device to access your device quickly.

You can exclude only full trusted devices that are on the local subnet.

To exclude a device from Intrusion Prevention scan, you must ensure that the IP address of the device never changes. Norton 360 uses IP addresses to identify devices on your home network. If the IP address of the device changes, Norton 360 cannot identify the trusted device that should be excluded from Intrusion Prevention scan.

You can exclude a trusted device from Intrusion Prevention scan only if you are sure that the device does not have any security threats.

When you apply Full Trust to a device and exclude it from Intrusion Prevention scan, the IP address and MAC address of the device are added to the Trust Control.

To exclude a device from Intrusion Prevention scan

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. Under **My Network**, in the **Network Security Map** row, click **Configure**.
4. If the **Network Security Overview** window appears, click **OK**.

5 In the **Network Security Map** window, do one of the following:
   - To edit the trust level of a device that is on your network, in the network map, click the device.
   - To edit the trust level of a device that you manually added, in the **Network Details** drop-down list, click **Trust Control**, and then click the device.
6 In the device details section, in the **Trust Level** row, click **Edit**.
7 In the **Edit Device Trust Level** window, click **FULL TRUST**.
8 At the bottom of the **Edit Device Trust Level** window, check **Exclude from IPS scanning**.
9 In the **Exclude from IPS Scanning** dialog box, click **Yes** to confirm.
10 Click **OK**.

Removing devices from the Network Security Map

The **Network Security Map** window lists the devices that are connected to your network. You can remove a device or a computer from the Network Security Map. You can purge all devices from the network map and create a new list of devices. For example, you can purge all the devices that were present in your previous network before you connect to a new network. Ensure that you disable Remote Monitoring before you purge the network map. Norton 360 cannot purge the network map when the Remote Monitoring is turned on. Also, ensure that you close the **Network Security Map** window before you purge the network map. You cannot purge the network map when the **Network Security Map** window is open.

Norton 360 purges the devices that you add manually in the Trust Control network depending upon their trust level. It does not purge the devices that have a trust level as Full Trust or Restricted.

When you remove an individual device, the online devices appear again the next time you open the Network Security Map. However, Norton 360 permanently removes the offline devices.

To remove an individual device

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**.
4. In the **Network Security Map** window, do one of the following:
   - To remove a device that is on your network, in the network map, click the device.
   - To remove a device that you manually added, in the **Network Details** drop-down list, select **Trust Control**, and then click the device.
5. On the left side of the **Network Security Map** window, under **Total in Network**, click the minus symbol.
6. In the confirmation dialog box, click **Yes**.

To purge the Network Security Map

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. Under **Network Security Map**, in the **Network Map** row, click **Purge**.
4. In the confirmation dialog box, click **Yes**.

Viewing the status of your wireless network

You can view the status of your wireless network in the **Network Security Map** window. The Network Security Map displays the status of your wireless network as secure or not secure. A secure network requires a strong wireless encryption. If your wireless network is not secure, you can turn on encryption on your wireless router.

For more information on how to secure your wireless network, on the left side of the **Network Security Map** window, click the **Why is it not secure** link. Follow the instructions.

You should only trust a wireless connection that is secure. Trusting a wireless connection that is not secure puts all of the devices on your network at risk.

To view the status of your wireless network

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**
4. On the left side of the **Network Security Map** window, view the status of your wireless network. Your wireless network statuses are:

Wireless Network Secure	Indicates that your wireless network is secure
Wireless Network Not Secure	Indicates that your wireless network is not secure

Viewing the device details

The Network Security Map lets you view the details of the computers that you remotely monitor. You can view the following details:

- The configuration status of your protection features, such as Auto-Protect, Intrusion Prevention, and Email Scanning
- The configuration status of your definition updates, such as Automatic LiveUpdate and Pulse Updates
- The version number of your Norton product
- The subscription status of your Norton product
- The configuration status of your transaction security, such as Identity Safe and Antiphishing

- The last five AntiVirus threats that are detected

To view the device details

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Network Security Map** row, click **Configure**
4. In the **Network Security Map** window, in the network map, click the device for which you want to see the details.
   You can view the details of only the computers that you remotely monitor.
5. In the device details section, next to **Category**, click **Details**.
6. In the **Device Details** window, view the details of the device.
7. Click **Close**.

Modifying the communication port for Network Security Map

The Network Security Map settings lets you configure the communication port number that Norton products use to communicate with each other over a network. By default, Norton products use 31077 as the communication port number.

If you change the communication port number of your Norton product, you must change it on every computer that is connected to your home network. In addition, when you find more computers that use the **Remote Monitoring Setup** process, ensure that the same port number is used on every computer.

Though you can modify the communication port number, it is recommended that you do not change this port number. If you change the communication port number, you must use a port number in the range of 1-65535.

To modify the communication port for Network Security Map

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **My Network**.
3. In the **Communication Port** box, type a new communication port number.
   You must use the same port number for each of the device that is connected to your **Network Security Map**.
4. Click **Apply**.
5. Click **Close**.

Keeping your PC tuned up

11

This chapter includes the following topics:

- About PC Tuneup
- About disk and file fragmentation
- Optimizing your permanent disks manually
- About using optimization efficiently
- About cleaning up disk clutter
- Running a scan to clean up disk clutter
- Running Registry Cleanup
- Running Diagnostic Report
- About Startup Manager

About PC Tuneup

Norton 360 offers total protection of your PC that includes PC Tuneup capability, which increases your PC performance. PC Tuneup keeps your computer tuned up for peak performance.

Norton 360 keeps your PC tuned up and running smoothly by using various techniques, such as optimizing your hard disk and deleting unused temporary files.

PC Tuneup detects and fixes common computer problems, cleans up unwanted cookies and files, and defragments the hard disk to optimize PC performance.

About disk and file fragmentation

Your PC's hard disk stores all of your files, applications, and the Windows operating system. Over time, the bits of information that make up your files gradually spread over the disk. This process is known as fragmentation. The more you use your computer, the more fragmented your disks become.

When a fragmented file is accessed, the disk performance is slower. The performance is slower because the drive head locates, loads, saves, and keeps track of all of the fragments of the file. If free space is also fragmented, the drive head might have to track adequate free space to store temporary files or newly added files.

Norton 360 optimizes your permanent disks to improve your PC's efficiency and speed. The optimization process rearranges the scattered file fragments into adjacent or contiguous clusters. When the drive head accesses all of the file data in one location, the file is read into the memory faster. Optimization also consolidates free space to avoid fragmenting newly added files. It adds extra space after major data structures so that they can grow without immediately becoming fragmented again.

Optimizing your permanent disks manually

Optimizing your PC's permanent disks can improve performance and reliability. Norton 360 automatically checks your permanent disks for fragmentation and optimizes them if they are more than 10 percent fragmented. You can always check the latest reports to see if optimization is necessary.

You can run Disk optimization only when disk has more than 15 percent of free space.

Some programs, such as movie-editing programs or programs that require large amounts of disk space, can work more efficiently if your disks are optimized. If you prefer not to wait until Norton 360 performs automatic optimization, you can optimize your disks manually.

Disk optimization does not run on PC with solid state hard drive.

To optimize your permanent disks manually

1. In the Norton 360 main window, click **PC Tuneup**, and then click **Run Disk Optimization**.
2. When the activity is complete, in the **Tuneup** window, click **Close**.

About using optimization efficiently

Norton 360 automatically optimizes the permanent disk in your PC as necessary and does not require you to take any action to accomplish that task. You can, however, adopt some practices that help Norton 360 perform automatic optimization more efficiently.

The following practices can help make automatic optimization more efficient:

Occasionally leave your PC turned on when you do not use the PC	Norton 360 performs disk optimization when your PC is idle. If you turn off your PC whenever you finish your work, Norton 360 cannot perform automatic optimization. If you turn off your PC during optimization, Norton 360 restarts the optimization process when you turn on your PC again.

Set a schedule for optimization	Norton 360 automatically optimizes the hard disk as needed. You can also set a schedule for optimization.
Remove the large files that you no longer need	Large files are often more fragmented than the smaller files. These fragmented files affect the performance of your computer.

About cleaning up disk clutter

Over time, the permanent disk in your PC can accumulate many temporary and unneeded files. Eventually, these files can significantly reduce the available disk storage space and affect the performance of your PC. Norton 360 automatically cleans up accumulated disk clutter.

The temporary files that clutter your PC can come from the following sources:

Software installations	When you install software on your PC, the installation process creates temporary files as part of the installation process. In some cases, the installer might not clean up these temporary files when the installation finishes.

Web browsing	When you browse a Web page, your browser downloads the text and graphics that comprise the contents of the page. When you finish viewing the page, the browser can leave the downloaded contents on your PC. The downloaded contents help to display the Web page more quickly if you view the page again. These browser files accumulate over time.
Program errors	During normal operation, some programs create temporary files to improve efficiency while you work. If a program ends unexpectedly because of a software error, those temporary files can be left behind.

Running a scan to clean up disk clutter

A cleanup scan searches your PC's permanent disk for temporary and unused files to improve performance and increase available disk space. Norton 360 automatically removes the temporary and the unused files from your PC.

Various activities, such as extensive Web browsing or a series of software installations produce temporary files. You can run a manual cleanup scan to remove the temporary files immediately.

To clean up your disk clutter

1 In the Norton 360 main window, click **PC Tuneup**, and then click **Run File Cleanup**.

2 When the activity is complete, in the **Tuneup** window, click **Close**.

Running Registry Cleanup

The Windows registry can contain the entries that refer to files that do not exist. Such broken registry items can slow down your computer. Registry Cleanup scans your computer and cleans any broken registry entries that it finds.

To run Registry Cleanup

1 In the Norton 360 main window, click **Tasks**.
2 In the **Tasks** window, under **PC Tuneup Tasks**, click **Run Registry Cleanup**.
3 When the activity is complete, in the **Tuneup** window, click **Close**.

Running Diagnostic Report

Norton 360 Diagnostic Report gathers information about your computer, which includes the operating system, programs, and hardware. You can use this report to find and fix the issues.

Norton 360 Diagnostic Report is a real-time report with a timestamp. Norton 360 does not generate this report automatically. You need to use the **Run Diagnostic Report** option and manually generate the report.

If Norton 360 finds any issues on your computer, you can use the **Fix Now** option to resolve the issues.

You can save, email, or print the report when needed for review.

To run Diagnostic Report

1 In the Norton 360 main window, click **PC Tuneup**, and then click **Run Diagnostic Report**.
2 When the activity is complete, view the details in **Diagnostic Report** window, and then click **Close**.

About Startup Manager

Some programs are configured to launch during startup of your computer. The number of startup items increases as you install new applications, and the time that is required to start your computer increases as a result. Startup Manager helps to manage the startup items on your computer. For any startup program that the Startup Manager lists, you can view the detailed information such as **Community Usage** and **Resource Usage**. You can also click the application name and view the File Insight details. These details would help you determine whether or not to enable an application during startup.

You can use Startup Manager to manage programs with the following extensions:

- Windows executable files (.exe)
- Windows System files (.sys)
- Dynamic link library files (.dll)
- ActiveX control files (.ocx)

Norton 360 displays the community usage details under the following conditions:

- When the **Norton Community Watch** option is turned on.

  See "Turning off or turning on Norton Community Watch" on page 33.
- When the **Metered Broadband Mode** option is configured to **No Limit** or **Critical Updates Only**.

  See "Defining the Internet usage of Norton 360" on page 298.

Startup Manager lets you view the list of programs that are included to the startup items. You can configure Startup Manager to run or not run these programs when your computer starts. You can also choose to delay the start of the programs and run them manually from the Startup Manager. This way, you can enhance the performance of your computer. You can disable a

program and measure the performance of your computer the next time you start your computer.

Norton 360 delays the start of the delayed programs by five minutes. The first delayed program in the **Startup Manager** window, starts five minutes after you start your computer. Every subsequent delayed program starts with a further delay of 10 seconds.

When you uninstall or if your Norton 360 expires, the programs that you had added to the Startup Manager are reset to their default startup setting.

Sometimes, you may see some startup programs missing from the startup list. Norton 360 removes a startup program from the list for the following reasons:

- When you disable a program that has a startup setting.
- When you update a program that can possibly reset all startup settings to default.
- When you use another program to manage your startup programs.
- When you edit the registry keys manually.

To add a startup item, you can open your Startup folder that is available in your Windows **Start** menu and add programs as required. For more information on adding programs in Windows Startup, go to Microsoft Technical Support Web site or Windows online Help.

Disabling or enabling startup items

Whenever you start your computer, there are some programs that automatically start and run in parallel. These programs are called startup items. The startup items increase the start time of your computer.

Startup Manager helps you manage the startup items of your computer efficiently. If you do not want a program to automatically start when you turn on your computer, you can disable the program using Startup Manager. You can also delay a startup item that you want to start at a later time.

To disable startup items

1. In the Norton 360 main window, click **PC Tuneup**, and then click **Run Startup Manager**.
2. In the **On/Off** column, uncheck a program that you do not want to automatically start when you turn on your computer.
3. Click **Apply** to save the changes.
4. Click **Close**.

To enable startup items

1. In the Norton 360 main window, click **PC Tuneup**, and then click **Run Startup Manager**.
2. In the **On/Off** column, check a program that you want to automatically start when you turn on your computer.
3. Click **Apply** to save the changes.
4. Click **Close**.

Managing startup items

Norton 360 Startup Manager monitors and lists the programs that automatically start when you turn on your computer. To reduce the start time of your computer and improve the performance, you can delay the start of some of the programs when you turn on your computer.

Norton 360 delays the start of the delayed programs by five minutes. The first delayed program in the **Startup Manager** window, starts five minutes after you start your computer. Every subsequent delayed program starts with a further delay of 10 seconds.

To delay startup items

1. In the Norton 360 main window, click **PC Tuneup**, and then click **Run Startup Manager**.
2. In the **Delay Start** column, check a program that you want to delay.
3. Click **Apply** to save the changes.
4. Click **Close**.

To run delayed startup items manually

1. In the Norton 360 main window, click **PC Tuneup**, and then click **Run Startup Manager**.
2. In the **Startup Manager** window, click **Run Delayed Items Now**.
3. Wait for the program to start, and then in the **Startup Manager** window, click **Close**.

Protecting your media and data

12

This chapter includes the following topics:

- About Norton Backup and Restore
- About backups
- About backup preparation
- About backup set
- Backing up your files
- Restoring files
- About Norton Backup Drive
- About solutions to the backup problems
- About online backup considerations
- Turning off or turning on backup
- Turning off or turning on backup setting options

About Norton Backup and Restore

The Norton Backup and Restore feature protects your important data and media files by regularly backing up the files. If something catastrophic happens to your PC, you can restore your valuable information from the backups that Norton 360 has made.

About backups

One of the most important ways to protect the valuable information on your PC is to back up your files regularly. In case you lose your data, Norton 360 lets you restore them later. For example, you accidentally erase an important file or your PC has a hardware malfunction that destroys some files. In this case, you can restore your lost files from your backup.

You can also use backup to keep your PC's permanent disk from becoming filled with old and seldom-used files. After you have backed up such files, you can remove them from your PC and restore them later if you need to use them again.

Norton 360 lets you to conveniently back up your files to any media that Windows recognizes as a storage drive. The backup destination may include external drive, network storage folders, CD, DVD, Blu-ray disc, iPod, flash drive, cameras, smart-phones, or a host of other devices.

For any file that you have backed up, Norton 360 lets you view the status through the icon overlays and the **Backup** tab in **Properties** page. The icon overlays on a file show the backup status of your protected files. You can view details such as the last backup time of each backup set in the **Backup** tab of the file Properties page. You can turn off these options if you do not want to view these icon overlays and the Backup details.

Norton 360 also provides a safe and a private online storage environment to which you can back up your files. The online storage location is different from the location where you normally store files in your PC. Disasters that damage or destroy your PC cannot harm your backups because they are stored in a different location. In addition, when you use the Norton 360 online backup, you can restore your files from any computer at any time. Norton 360 must be installed in the PC to access your Norton Account.

No matter which backup method you choose, you can always add or remove items from the set of files that you select to back up. You can add or remove an individual file from the backup sets by using the shortcut menu that appears when you right-click a file.

About backup preparation

After you install Norton 360, you must configure Norton 360 backup to back up your important files on your computer. You can back up your important files with Norton 360 either automatically or at a time that you specify. You can always change the backup settings you initially make.

Choose the following settings when you make a backup:

Summary	You can perform the various tasks that are related to the backup sets such as creating, deleting, and renaming backup sets. You can also preview the details that are related to any particular backup set such as the size and the available files.

What	You can choose from a variety of file types, such as photos, documents, and music. You can also specify individual files. You have the following options: ▪ **Sources** Lets you select a source from which you want to back up your files. Norton Backup is comprehensive or short depending on the locations that you select. ▪ **File Types** Lets you include or exclude a backup file category. You can add a file or a folder to the backup or exclude a file or a folder from the backup. You can also use **Add or exclude files and folders** option to view the added and excluded files and folders. In addition, you can use the **Edit File Type** option to edit file extensions within each file category. When you check **Edit File Type**, you can add, edit, or remove the file extensions in each Backup category by using the **Configure** option.

Where	

	You can choose any storage location that Norton 360 offers for your backup location, depending on your PC and the connected devices. You can choose to store your backups on external media, such as CD, DVD, Blu-ray disc, or iPod. You can also store your backups on a network drive, removable flash memory drive, or permanent disk in your PC. Backing up your files to a location where your source files are available is not safe. You may lose your data during hardware malfunctions. You can delete the previously backed-up files. You can also decide if you want to verify your backups by checking the **Verify backup** option. Norton 360 also provides a secure online backup service that you can use to store your backed-up files in a safe location on the Internet. This service protects your information even if something catastrophic happens to your computer. To use the **Secure Online Storage** option, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network**

	option is available in the **Settings** window.
When	You can have Norton 360 back up your files when your computer is idle. You can also set a regular backup schedule or manually back up your files.

When you use the **Secure Online Storage** option for the first time, Norton 360 needs to be activated. To activate the Secure Online Storage, click the **Click here to activate your Secure Online Storage** link. The online backup service that is provided with the Norton 360 requires you to create a Norton Account. When you back up files online, Norton 360 requests your Norton Account name and password, which prevents unauthorized access to your backed-up files.

Before Norton 360 runs a backup, it examines the files on your computer so that it can back up your files more efficiently. During this initial examination, Norton 360 counts the number of files that may need to be backed up. Norton 360 also records the types and sizes of those files. This process usually takes no more than a few minutes the first time you run a backup.

About backup set

Norton 360 lets you create multiple sets of backup configurations. The configuration is a set of rules and is called a backup set. You can specify the files that you intend to back up, the backup destination, and the time when you want to back up your files. You can use multiple backup sets to back up different combinations of files or file categories to different locations.

Multiple backup set creation helps you to use your limited Secure Online Storage judiciously. For example,

you can create a backup set to back up your picture files and music files to a CD. You can also create another backup set to back up your Microsoft Office documents and your financial files to your Secure Online Storage.

To use **Secure Online Storage** option, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

You can do the following tasks:

- You can create multiple backup sets with different set of rules. For example, you can create a backup set to back up your pictures to your local fixed disk. You can also create another backup set to back up your videos to a CD. You can configure different schedules for each backup set.
- You can modify a backup set to include or exclude files or file categories or to use another backup destination to back up your files. You can change the schedule of a backup set. You can also rename a backup set if the name does not describe the backup set after you modify the rules.
- You can delete a backup set if it is no longer needed. You can create a new backup set to start backing up your files from the beginning.

The **Summary** tab of the **Manage Backup Sets** window displays the set of rules that you have configured for each backup set. You can select a backup set from the **Backup set name** drop-down list to view the rules. This way, you can keep a record of the files or file categories that Norton 360 backs up to different destinations. You can also modify the rules if required. In addition, you can view the date and time of the last backup activity for a backup set.

Creating a new backup set

You can create multiple backup sets with different configurations. For example, you can create a backup

set to back up your pictures to your local fixed disk. You can create another backup set to back up your videos to a CD. You can also configure different schedules for each backup set.

When you create a new backup set, Norton 360 applies the default configuration for the backup set. You can change the configuration if the default configuration does not meet your needs.

You can identify each backup set with a backup set name. The default name of a backup set is **DefaultSet**. You can save a backup set with the default name as well. But, whenever you create a new backup set, you must provide a name for the backup set. The maximum character length of a backup set name is 32 alphanumeric characters. You cannot create more than 10 backup sets.

To create a new backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **Summary** tab, under **Things you can do**, click **Create new backup set**.
3. In the window that appears, type a name for your backup set, and then click **OK**.
4. On the **What** tab, under **File Types**, select a file category.
5. In the **Manage Backup Sets** window, click **Save Settings**.

Modifying or renaming a backup set

When you create a new backup set, Norton 360 applies the default configuration for the backup set. You can change the configuration if the default configuration does not meet your needs.

You can modify a backup set to include or exclude files or file categories or choose another backup destination to back up your files. You can change the schedule of a backup set. You can also rename a backup set if the

name does not describe the backup set after you modify the configuration.

The maximum character length of a backup set name is 32 alphanumeric characters.

To modify a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **Summary** tab, in the **Backup set name** drop-down list, select the backup set that you want to modify.
3. Under **Backup Set Summary**, view the details of the backup set, and do the following:
   - To include or exclude files or file categories in a backup set, click **What**, and change the settings.
   - To change the backup destination, click **Where**, and change the settings.
   - To change the backup schedule, click **When**, and change the settings.
4. In the **Manage Backup Sets** window, click **Save Settings**.

To rename a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Set**.
2. On the **Summary** tab, in the **Backup set name** drop-down list, select the backup set that you want to rename.
3. Under **Things you can do**, click **Rename backup set**.
4. In the window that appears, change the name of the backup set, and then click **OK**.
5. In the **Manage Backup Sets** window, click **Save Settings**.

About backup file categories

When Norton 360 performs a backup, it first examines the permanent disk of your PC for files to back up and

sorts them into various categories. It then backs up the files that fall into these categories.

Norton 360 uses the following file categories:

Pictures	This category includes, but is not limited to: Photographic JPEG and JIFF images (.jpg, .jpeg, .jpe, .jP2, .j2k, .j2c, .jpf); Graphic Interchange Format image files (.gif); Bitmap Graphics files (.bmp, .pct); Tagged Image Format files (.tif, .tiff); Adobe PhotoDeluxe images (.pdd); Windows Metafile (.wmf); Portable (Public) Network Graphic files (.png); Photoshop files (.psd); Macintosh Quickdraw/PICT Drawing files (.pict); Encapsulated PostScript files (.eps); MS Foxpro Screen files (.sct); Run Length Encoded Bitmap files (.rle); Device-Independent Bitmap Graphic files (.dib); Borland JBuilder Project files (.jpx); Japan Picture Format files (.jpc); Image Alchemy HSI Temporary Raw Bitmap files (.raw); Pixar Picture files (.pxr); CAD files (.vda); Pixar Picture File (.pxr); TARGA File (.tga); Adobe Illustrator Vector Graphic (.ai); Kodak Photo CD (.pcd); Kodak RAW Bitmap Image (.kdc); Adobe InDesign Document (.indd); Paint Shop Pro Image (.psp); Corel Vector Graphic Drawing (.cdr); and Targa Bitmap files (.icb, .vst).

Music	This category includes, but is not limited to: MPEG Audio Stream, Layer III files (.mp3); MPEG-4 Video files (.mp4); MPEG-4 Audio Layer files (.m4a); Apple Protected AAC files (.m4p); Real Networks RealMedia Streaming Media files (.ra); RealMedia Streaming Media files (.rm); RealMedia Metafile files (.ram); MIDI files (.rmi); MS Windows Media Audio files (.wma); MPEG-2 Advanced Audio Coding files (.aac); Monkey's Audio Lossless Audio Compression Format files (.ape); Free Lossless Audio Codec files (.flac); Waveform Audio files (.wav); MP3 Playlist files (.m3u); Musical Instrument Digital Interface MIDI Sound files (.mid; .midi); Fast Tracker 2 Extended Module files (.xm); ScreamTracker v3 Sound files (.s3m); MPEG Audio Stream, Layer I (.mp1); Windows Media Player Playlist (.wpl); Playlist (.pls); Audio Codec 3 File (.a3c); Audio Interchange File Format (.aif, .aifc, .aiff); and MPEG Audio Stream, Layer II (.mp2).

Financial Files	This category includes, but is not limited to: Microsoft Money files (.mny, .mn1, .mn2, .mn3, .mn4, .mn5, .mn6, .mn7, .mn8, .mn9, .mn10, .mn11, .mn12, .mn13, .mn14, .mn15, .mbf); TurboTax Tax Return files (.tax); H&R Tax Return files (.t01, .t02, .t03, .t04, .t05, .t06); TaxACT files (.ta0, .ta1, .ta2, .ta3, .ta4, .ta5, .ta8, .ta9); QuickBooks files (.qba, .qbb, .qbi, .qbw, .qbx, .qph, .qdf, .qdb, .qif, .qsd, .qel, .qph, q00, q01, .q02, .q03, .q04, .q05, .Q98); Olicom Fax files (.ofx); Quicken Data File (.qdt); Simply Accounting File (.sdb); and Open Financial Connectivity files (.ofc).

Video	This category includes, but is not limited to: Microsoft Windows Media files (.wmv); Apple QuickTime Video Clip files (.mov); MPEG 1 System Stream files (.mpg, .mpeg); Macromedia Flash Format files (.swf); Audio Video Interleave files (.avi); MS Advanced Streaming Format files (.asf); Beijer E-Designer files (.mpa); MPEG Movie Clip files (.mpe); MPEG-4 Video files (.m4v); Digital Video File (.dv); Ogg Vorbis Compressed Video File (.ogm); Open Media Format File (.omf) MPEG-1 Video File (.m1v); MPEG-2 Program Stream Format File (.m2p); MPEG-2 Video Only File (.m2v); QuickTime Movie (.moov); MPEG-1 Video File (.mpv); QuickTime Movie (.qt); VDOScript File (.vdo); and DVD Video Movie File (.vob).

Office Documents	This category includes, but is not limited to: Microsoft Word documents and templates (doc, .dot); Microsoft Excel Worksheet and templates (.xls, .xlt, .xlam); Microsoft PowerPoint Presentation and Slideshow files (.ppt, .pps); Microsoft Project files (.mpp); Adobe Acrobat files (.pdf); Text files (.txt); PostScript files (.ps); HyperText Markup Language files (.htm, .html); Microsoft HTML documents (.mht); WildTangent Branded .PNG files (.wpg); Comma-Separated Variables text files (.csv); and WordPerfect PC Suite documents (.wpd).
Email	This category includes, but is not limited to: Microsoft Outlook Personal Folder files (.pst); Microsoft Exchange Mail messages (.msg); Microsoft Outlook Express E-mail or Windows Mail (.dbx); Netscape Mail E-mail Message files (.snm); Media Stream Broadcast (.msb); Mailbox Message File (.mbx); Microsoft Outlook Rules Wizard File (.rwz); Microsoft Outlook Express Electronic Mail (.eml); First Reader Saved Message Folder (.fol); and (.MsMessageStore).

Contacts	This category includes, but is not limited to: Microsoft Outlook Address Book files (.wab); Microsoft Personal Address Book files (.pab); Palm Address Book files (.aba); Beijer E-Designer files (.mpa); Palm Date Book files (.tda); vCard files (.vcf); Microsoft Outlook Address Book (.oab); Microsoft Phonebook (.pbk); Palm DateBook File (.dba); and Sharp Organizer Telephone Bank (.ozp).
Internet Favorites	This category includes, but is not limited to: Internet Location files (.url) that appear on the **Internet Explorer Favorites** menu.
Other File Types	This category includes the files that you specifically add to the backup. The category also includes the files that Norton 360 cannot add to any of its file categories.

About backup file extensions

A file extension is a string of characters that is appended to the name of a file and is used to identify the file format. Norton 360 uses the file extension to back up the files that are present on your computer into different categories. Each backup file category contains a list of default file extensions. When you run a backup, Norton 360 identifies the files that are based on the file extensions and backup file categories. For example, if you want to back up the documents with a

.fm file extension in the Office Documents category, you can add the .fm file extension to the category.

The **Edit File Type** option on the **What** tab of the **Manage Backup Sets** window lets you add, edit, or remove file extensions in each backup category. When you check **Edit File Type**, the **Configure** option that appears next to each backup category lets you edit file extensions in that category.

You can use the **Edit File Type** option on the **What** tab of the **Manage Backup Sets** window to do the following:

- You can view the file extensions that are already listed in a backup file category.

  This option helps to ensure that the list has the extensions of files that you intended to back up.
- You can add a file extension to the list or edit a file extension that is present in the list.

  This option helps to ensure that the next time when you run backup, Norton 360 must back up the files with the extensions that you added.
- You can remove a file extension from the existing list or a file extension that you added.

  This option helps to ensure that Norton 360 does not back up the unintended files, the next time you run backup.
- You can reset a file category to its default file extensions.

  This option helps to restore the changes you made to a backup file category.

The file extensions are independent of a backup set. If you change a file extension in a backup file category, the change applies to all backup sets.

Adding or editing a file extension in a backup file category

Each backup file category contains a list of file extensions. However, you can add a file extension to a backup file category. Norton 360 identifies the files

with the file extension that you added and backs them up to that file category. For example, if you want to back up the documents with a .fm file extension in the Office Documents category, you can add the .fm file extension to that category.

You can also edit an existing file extension or a file extension that you added.

The maximum character length of a file extension is 10 characters.

To add a file extension to a backup file category

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, next to **File Types**, check **Edit File Type**.
3. Under **File Types**, next to a file category, click **Configure**.
4. In the window that appears, click **Add New**.
5. Type the file extension that you want to add.
6. Click **OK**.
7. Click **Save**.

To edit a file extension in a backup file category

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, next to **File Types**, check **Edit File Type**.
3. Under **File Types**, next to a file category, click **Configure**.
4. In the window that appears, select the file extension that you want to edit, and then click **Edit**.
5. Edit the file extension.
6. Click **OK**.
7. Click **Save**.

Removing a file extension from a backup category

Each backup file category contains a list of file extensions. However, you can remove a default file extension or a file extension that you added to a backup file category. Norton 360 identifies the files with the file extension that you removed and does not back them up the next time that you run backup. For example, you do not want to back up the documents with a .rtf file extension in the **Office Documents** category. In this case, you can remove the .rtf file extension from that category.

To remove a file extension from a backup category

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, next to **File Types**, check **Edit File Type**.
3. Under **File Types**, next to a file category, click **Configure**.
4. In the window that appears, select the file extension, and then click **Remove**.
5. Click **Save**.

Resetting a backup category to default file extensions

You can reset a file category to its default list of file extension. When you reset a file category, Norton 360 restores the default file extension that you removed previously and remove the file extensions that you added.

To reset a backup category to default file extensions

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, next to **File Types**, check **Edit File Type**.
3. Under **File Types**, next to a file category, click **Configure**.

4 In the window that appears, click **Reset Defaults**.
5 Click **Save**.

Deleting previously backed up files

You can delete the files that you backed up previously from your backup location. You can also delete the files if the files are no longer useful for you and you have a limited space on your backup location. You can also delete backed up files if you changed the file category for a backup set. You may want to delete previously backed up files before you run a backup.

You can delete the previously backed up files from the following locations:

- **Summary** tab
- **Where** tab

When the backed up files are deleted, the backup details of the files that belong to the backup set that you delete also changes. For example, the icon overlays and the Backup tab in the file properties of the file no longer appear.

You cannot delete a backup set if only one backup set is available.

You can also uncheck the backup category if you no longer want to back up the files that you deleted.

Deleting previously backed up files is particularly helpful if you want to free some space on your Secure Online Storage.

To delete files from your online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

To delete previously backed up files from the Summary tab

1 In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.

2 On the **Summary** tab, in the **Backup set name** drop-down list, select the backup set that you want to delete.
3 Under **Things you can do**, click **Delete backup set**.
4 In the **Delete Backup Set** window, select one of the following:

Delete backup set	Lets you remove the backup set.
Delete backup set and files	Lets you remove the backup set and the files that are available in the backup set.

5 Click **Yes** to confirm.

To delete previously backed up files from the Where tab

1 In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2 On the **Where** tab, click **Delete Backed up Files**.
3 In the window that appears, in the drop-down list, select the backup set from which you want to delete the previously backed up files.
This window appears when you have more than one backup set.
4 Click **OK**.
5 In the window that appears, in the left pane, select the file category that contains the files.
You can also select the **Folders** category to select the folders that you want to delete.
6 Check the files that you want to delete.
7 To view the files that you selected, on the left pane, click **Selected Files**.
8 Click **Delete Selected**.
9 In the confirmation dialog box, click **Yes**.
10 Click **Close**.

Adding files and folders to a backup set

You are not limited to backing up the files that Norton 360 automatically detects and places into its file categories. You can add files to the set of files to be backed up, and you can exclude files from being backed up as well.

Norton 360 lets you select a file or folder from your computer that you want to include in your backup. The **Add or exclude files and folders** option on the **What** tab in the **Manage Backup Sets** window provides you the options to add files and folders to a backup set.

You can also right-click a file or a folder and add it to a backup set using the Norton 360 option on the shortcut menu. The shortcut menu is available after you configure your backup and when the **Manage Backup Sets** window and the **Restore Files** window are closed. When you add a file to the backup set, Norton 360 lists the information in the window that appears when you click **Add or exclude files and folders** option. You can view all the files and folders that you added to the backup.

You can also remove an addition from the list of items that is included or excluded from backup by using the **Remove from list** option. This option is available in the window that appears when you click **Add or exclude files and folders**.

To add files to your online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

To add a file to a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, click **Add or exclude files and folders**.
3. In the window that appears, click **Include File**.

4 In the file selection window that appears, navigate to file that you want to add, click to select it, and then click **Open**.
5 Click **OK**.
6 In the **Manage Backup Sets** window, click **Save Settings** to save the settings.

To add a folder to a backup set

1 In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2 On the **What** tab, click **Add or exclude files and folders**.
3 In the window that appears, click **Include Folder**.
4 In the folder selection window that appears, navigate to the folder that you want to add, and then click **OK**.
5 Click **OK**.
6 In the **Manage Backup Sets** window, click **Save Settings** to save the settings.

To add a file or folder to a backup set in Windows Explorer

1 In Windows Explorer, right-click the file or folder, select **Norton 360 > Add to Backup**.
The **Add to Backup** option in the shortcut menu is enabled only after you configure your backup and when the **Manage Backup Sets** window and **Restore Files** window are closed.
2 Click the backup set to which you want to add the file or the folder.

Excluding files and folders from a backup set

Norton 360 lets you exclude backing up the files that Norton 360 automatically detects and places into its file categories or a complete file category. The **Add or exclude files and folders** option on the **What** tab in the **Manage Backup Sets** window provides you the options to exclude files and folders to a backup set.

You can exclude a file or folder from the backup set from Windows Explorer by using the shortcut menu. The shortcut menu is available after you configure your backup and when the **Manage Backup Sets** window and the **Restore Files** window are closed. When you exclude a file from the backup set, Norton 360 lists the information in the window that appears when you click **Add or exclude files and folders** option. You can view all the files that you excluded from the backup.

You can also remove an exclusion from the list of items that is included or excluded from backup by using the **Remove from list** option. This option is available in the window that appears when you click **Add or exclude files and folders**.

To exclude a file from a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, click **Add or exclude files and folders**.
3. In the window that appears, click **Exclude File**.
4. In the file selection window that appears, navigate to the file that you want to exclude, and then click **Open**.
5. Click **OK**.
6. In the **Manage Backup Sets** window, click **Save Settings** to save the settings.

To exclude a folder from a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **What** tab, click **Add or exclude files and folders**.
3. In the window that appears, click **Exclude Folder**.
4. In the folder selection window that appears, navigate to the folder that you want to exclude, and then click **OK**.
5. Click **OK**.

6 In the **Manage Backup Sets** window, click **Save Settings** to save the settings.

To exclude a file or folder from a backup set in Windows Explorer

1 In Windows Explorer, right-click the file, click **Norton 360 > Exclude from Backup**.
The **Exclude from Backup** option in the shortcut menu is enabled only after you configure your backup and when the **Manage Backup Sets** and the **Restore Files** windows are closed.

2 Click the backup set from which you want to exclude the file or the folder.

About backup locations

Norton 360 can back up your files to several kinds of storage locations. The speed, safety, and quantity of your backup depend on the choice of your location. No one backup location is the best in all situations and for all users.

You can choose any storage location that Norton 360 offers for your backup location, depending on your PC and the connected devices. Use the information in the

following table to choose a location that best meets your needs for safety, speed, and storage capacity:

Secure Online Storage	

	Your subscription to Norton 360 comes with an allocation of storage space on a secure server that is located on the Internet. This location is the safest, most secure backup choice available because it stores your information in a remote location. As a consequence, even the disasters that might damage or destroy your PC cannot affect your backups. Online backups can take place automatically, as long as your PC has an active Internet connection. However, you require a reasonably fast Internet connection. You can configure the Internet bandwidth that backup uses to back up your files using **Bandwidth Throttle** on the **Where** tab of the **Manage Backup Sets** window. You can alter the following bandwidth throttle states: ▪ **Fastest (recommended)** ▪ **High usage** ▪ **Moderate usage** ▪ **Low usage** You can buy more online storage space whenever you want. To use the **Secure Online Storage** option, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

C: (Local Fixed Disk)	This choice backs your files up to a special folder on drive C of your PC. Backing up to drive C is very quick and convenient, and is only limited to the amount of free space available on your drive. You can run automatic backups with this choice. Backing up to drive C is a convenient but an unsafe backup method. Any mechanical problem that the drive might experience can damage both your original files and your backups. If you use drive C for quick and automatic backups, you must back up your files occasionally to a different drive or another location.
Other internal or external drive	This choice provides for fast, convenient backups. You can run automatic backups and always have access to your backed up files as long as the drive is connected to your PC. Although using another drive is safer than using drive C, doing so still leaves your data at risk from any PC hardware malfunctions. If you choose to back up to another drive, you should also back up your files occasionally to some other location.

CD, DVD, or Blu-ray discs	

	This choice requires that you have recordable CDs, DVDs, or Blu-ray discs and an optical drive in your PC to record on those discs. You must be present to insert and remove discs when requested. Therefore, you cannot select automatic scheduling of backups when you back up to CDs, DVDs, or Blu-ray discs. Backing up to CDs, DVDs, or Blu-ray discs is slower than backing up to other media. Backing up to CDs, DVDs, or Blu-ray discs is also less convenient because you must be present during the backup. By using Norton 360, you can back up your data to any of the following optical media types if your optical drive supports them: ■ CD-R ■ CD-RW ■ DVD+R ■ DVD-R ■ DVD+R DL ■ DVD-R DL ■ DVD+RW ■ DVD-RW ■ DVD RAM ■ BD-R ■ BD-RE You should store your backup discs in a safe place elsewhere to provide protection against a disaster that occurs at your computer's location. When you select the CD or the DVD Drive as the backup

	location for the first time, Norton 360 prompts you to configure the optical backup drive on your computer. Norton 360 lets you install the optical driver.
Network drive	You can use this choice if your PC is connected to a local network that offers a storage location to which you have access. Depending on the speed of your network, this choice can be almost as fast as backing up to an internal drive or external drive. This choice does not appear if your PC is not connected to a network that offers a storage device to which you have access. To back up your data to an external network drive, you must map the external network drive to your computer. When you map a drive, you must also specify a drive letter for the connection.

Flash drive and removable storage devices, including iPod	Flash drives and the other data storage devices that are attached to your PC can also serve as backup locations. Norton 360 displays such devices as external disk drives. If such a device is always attached to your PC, you can use it for automatic backups. The amount of storage space that is available on these devices can be less than on hard disks. If you use a flash drive for backups, you should also back up your files occasionally to another storage location.

Choosing a backup location

Norton 360 provides several kinds of storage locations for backups. You can choose a different location if your backup needs change or if you want to store your backups in several locations for added security.

When you select Secure Online Storage as the backup location, Norton 360 prompts you to register to your Norton Account. You must be connected to the Internet to register to your Norton Account.

To use Secure Online Storage as a backup location, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

You must activate your Norton 360 with a valid license key to use the online storage space.

To choose a backup location

1. Make sure that the device to which you want to back up your data is connected to your PC and turned on.
2. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.

3 On the **Where** tab, select the location and device where you want your backups to be stored.
If the device or location does not appear on the list, click **Refresh List**.
4 Click **Save Settings**.

Installing optical backup driver

Norton 360 offers several storage location options for backups. You can choose a different location if your backup needs change or if you want to store your backups in several locations for added security.

If you want to back up your important files and data to a CD or DVD Drive, you must configure the optical backup drive on your computer. The optical backup drive helps you read or write data on optical discs.

When you select CD or DVD Drive as the backup location for the first time, Norton 360 prompts you to configure the optical backup drive on your computer. Norton 360 lets you install the optical driver.

When you install optical backup driver, you must insert and remove discs when prompted. Therefore, you cannot select automatic scheduling of backups when you back up to CDs, DVDs, or Blu-ray discs for the first time. When the backup is complete, you can click **View Details** in the **Backup** window to view the status of your last backup.

To install optical backup driver

1 In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2 On the **Where** tab, select the **CD or DVD Drive** option, and then click **Run Backup**.
3 In the dialog that appears, click **OK**.
4 When you are prompted, insert a blank CD or DVD into the CD-ROM drive and click **OK**.
You can view the progress of the backup in the **Backup** window.
5 When the backup is complete, click **Close**.

Viewing or changing a backup schedule

Norton 360 lets you schedule backups when it is convenient for you. You can schedule your backups to run late at night or whenever you know that your computer is not needed for any other activity.

You have the following backup schedule choices:

Automatic (Recommended)	Choose this option to back up your computer when it is turned on but not otherwise in use. This choice is the recommended choice for most users. Norton 360 checks your computer to be idle every four hours to run an automatic backup. Note that the backup location must be available at the time that the automatic backup takes place. You cannot back up your data to a CD or DVD if you select this option.
Weekly	Choose this option to pick one or more days of the week, and the time of day, for your backups to occur.
Monthly	Choose a specific day of the month, and specific time of a day, for your backups to occur. Check **Run only at idle time** to run an automatic backup only at idle time. Norton 360 checks to see if your computer is idle every four hours.

Manual Schedule	Choose this option to have Norton 360 backup your files only when you start the backup yourself.

Your computer's performance is maximized if you schedule to perform your critical operations when your computer is idle. When you schedule backup weekly or monthly and check the **Run only at idle time** option, Norton 360 backs up your files when your computer is idle. Symantec recommends you to check the **Run only at idle time** option to experience better performance of your computer.

To view or change a backup schedule

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **When** tab, under **Schedule**, select an option to view or change the backup schedule.
3. Click **Save Settings**.

Deleting a backup set

You can delete a backup set if it is no longer needed. You cannot delete a backup set if only one backup set is available. However, you can create a new backup set before you delete the old backup set.

When a backup set is deleted, the Backup details of the files that are included in that backup set also change. For example, the icon overlays and the **Backup** tab in the file properties of the file no longer appear.

Deleting a backup set is particularly helpful if you want to free some space on your Secure Online Storage.

To delete a backup set from your online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

To delete a backup set

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **Summary** tab, in the **Backup set name** drop-down list, select the backup set that you want to delete.
3. Under **Things you can do**, click **Delete backup set**.
4. In the **Delete Backup Set** window, select **Delete backup set** option.
5. In the confirmation dialog box, click **Yes**.

To delete a backup set and files

1. In the Norton 360 main window, click **Backup**, and then click **Manage Backup Sets**.
2. On the **Summary** tab, in the **Backup set name** drop-down list, select the backup set that you want to delete.
3. Under **Things you can do**, click **Delete backup set**.
4. In the **Delete Backup Set** window, select **Delete backup set and files** option.
   The **Manage Backup Set** window shows the progress of the backed files that are being deleted from your selected backup set.
5. Click **Yes** to confirm.

Backing up your files

After you provide Norton 360 with your preferred backup settings, running a backup is very easy. In fact, if you scheduled all backup sets to run backups automatically, you do not need to do anything at all. Norton 360 performs automatic backups for all backup sets when your PC is turned on but not engaged in performing any other tasks. However, Norton 360 does not back up your files automatically if the backup destination is a CD, DVD, or Blu-ray disc. Backing up to these destinations needs your intervention.

Whether you have set Norton 360 to back up your PC automatically or not, you can always run a backup. For example, you have added or modified important files and you want to be sure they are safe. In this case, you can run a backup manually. You can also run a backup at the end of the day if you do not want to wait for an automatic backup to occur.

You can view the details of your backup activity under the backup category in the **Security History** window.

To back up your files

1. In the Norton 360 main window, click **Backup**, and then click **Run Backup Now**.
2. Follow any instructions for performing the backup that Norton 360 provides.
   For example, if you choose to back up your files to CDs, then Norton 360 asks you to insert a recordable CD.
3. In the **Backup** window, click **Close**.

Restoring files

The reason to have a good backup is to restore your files from the backup if the need arises. Norton 360 provides an easy method to restore your backed-up files.

By default, Norton 360 displays the backup location of the most recent backup set you ran and the original locations of the files.

To restore files from online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

When you restore files, you can change any of the following settings:

Restore From	You can choose any of the backup sets to restore the files. If you backed up your data in an external media, you must connect it to your computer to restore those files. Norton 360 lists all the backup sets that you ran backup for and that your PC can currently detect.
Files	You can restore the backed up files in a backup set that you selected. You can use the **Search** option to search for files by name and add the selected file to restore. You can also check the **Restore All Files and Categories** option next to the **Files** heading to select all file categories. In addition, you can browse for backed up files based on file categories and folders by using the **Browse for Files and Folders** option. You can filter the backed up files in a backup set by the backup file categories.

Restore To	You can restore to the original locations of the files, or navigate to a new location where you can restore your files. Norton 360 displays the total number of files and the total size of the files that you have selected for restoration. If files with the same name are present at the original location, the files that you restore replace those files.

If you backed up files to CDs or DVDs, do not restore files by copying them directly to your PC from the backup disks. When Norton 360 backs files up to CDs or DVDs, it sometimes has to split files between two discs. Directly copying a file back from a disc, therefore, may only copy part of the file. Such a file appears to be damaged when you try to use it. Instead, let Norton 360 restore your files for you.

To restore files

1. In the Norton 360 main window, click **Backup**, and then click **Restore Files**.
2. In the **Restore Files** window, do one or more of the following:
   - Under **Restore From**, change where to restore from.
   - Under **Files**, specify what to restore.
   - Under **Restore To**, change where to restore the files to.
3. Click **Restore Files**.
4. Follow the on-screen instructions to finish restoring your files.

Choosing where to restore files from

When Norton 360 restores files, it displays the backup location of the most recent backup set you ran. You can change the location to restore files from a different backup location. For example, you have backed up files to drive C and then later backed up files to CDs. You can then choose to restore files from either drive C or from the CDs.

To restore files from online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

To choose where to restore files from

1. In the Norton 360 main window, click **Backup**, and then click **Restore Files**.
2. In the **Restore Files** window, under **Restore From**, click **View All**.
3. In the window that appears, click the backup set that you want to restore, and then click **OK**.
   If the backup set is not visible, make sure that the media in which you had backed up your files is connected, and click **Refresh List**.
   If you have activated online backup, the window also contains the backup set that contains the files that you backed up online from another computer. For example, you can view the backup set containing the files that you backed up from your home computer. However, the other computer must have Norton 360 registered with the same Norton Account.
4. Make any other necessary changes to your restore settings, and click **Restore Files**.
5. Follow the on-screen instructions to finish restoring your files.

Selecting files to restore

When you restore backed-up files with Norton 360, you might not need to restore all the files from a backup. You can restore the files that may have been damaged, accidentally erased, or modified incorrectly. Norton 360 provides several ways for you to select only the files that you need to restore.

When you click the **Browse for Files and Folders** option, you can view a list of all the backed-up files. You can easily select the files that you want to restore by checking them. You can filter the files by its categories available in the left pane in the **Restore Files** window.

The various options that are available under **Category** in the left pane of the window are:

All file types	You can view all the backed-up files in a backup set.
File Categories	You can view all the file categories in the left pane that you have previously backed up. When you click a file category, you can view all the backed-up files of that file category in the right pane.
Folders	You can view all the backed-up folders containing files available in a backup set.
Selected Files	You can view all the files and folders that you select to restore.

You can also search for a particular file by using the **Search** option. You can exclude each item in the right pane if you want to exclude it from restoration by unchecking it.

You can use any of the following methods, and you can combine methods, to select files to restore:

Restore all files and categories	You can restore all the backed-up files without excluding any file within a backup set.
Restore files by searching	You can search by file name, or by part of a file name from the list of backed up files and restore them. You can also use wildcard characters, such as asterisks (*) or question marks (?) to search file names or folder names. For example, you can type *.doc to search all the Microsoft Word documents.
Restore individual files within a file category	You can see a list of the files that are included in each file category, and choose which of those files to restore.

You can select the files and the file categories that you want to restore in the **Restore Files** window.

To select all the backed-up files to restore

1. In the Norton 360 main window, click **Backup**, and then click **Restore Files**.
2. In the **Restore Files** window, next to **Files**, check **Restore All Files and Categories**.
   All of the backed-up files and folders in the backup set get selected for restore.

To select files to restore by searching

1. In the Norton 360 main window, click **Backup**, and then click **Restore Files**.

2 Under **Files**, in the **Search** text box, type all or part of a file name, or the extension of the file.

3 Click **Search**.
The window that appears displays the file names that contain the text that you typed.

4 Check the files that you want to restore, and then click **OK**.

5 Repeat steps 2 through 4 to add more files to the list of those that Norton 360 restores.

To select an individual file within a file category to restore

1 In the Norton 360 main window, click **Backup**, and then click **Restore Files**.

2 In the **Restore Files** window, under **Files**, click **Browse for Files and Folders**.

3 In the left pane, under **Show Results for**, click a file category from which you want to restore files.

4 In the right pane, do one of the following:

- Check the files that you want to restore.
- If you want to restore all the files in that category or folder, check the check box in the header close to **Backup Item**.

5 Repeat steps 3 through 4 to add more files to the list of those that Norton 360 restores.
You can use the **Selected Files** option in the left pane under **Show Results for** to view all the selected files that you want to restore.

6 Click **OK**.

Choosing a restore destination

When you restore files from a backup, you can choose where Norton 360 places the restored files. You can restore the files to a separate folder of your choice or their original location. By default, Norton 360 selects the original locations of the files.

Restoring files to their original locations deletes newer versions of the same files that are stored in those locations. If you do not want to replace those files with the restored files, you must move the newer versions somewhere else before you restore. You can also restore them to a different location.

You can change the restore destination from any computer at any time.

Some drives use older Windows file systems, such as FAT-16 or FAT-32, which cannot store files larger than 4 GB. For such large files to restore, make sure that your restore destination is formatted with a file system that supports large files, such as NTFS.

To change a restore destination

1. In the Norton 360 main window, click **Backup**, and then click **Restore Files**.
2. In the **Restore Files** window, under **Restore To**, click **Change**.
3. In the window, click **New Location**.
4. Do one of the following:
   - Type a restore location in the space provided.
   - Click **Browse**, use the browse window to navigate to the location to which you want to restore files, and then click **OK**.
5. Make any other necessary changes to your restore settings, and then click **Restore Files**.
6. Follow the on-screen instructions to finish restoring your files.

About Norton 360 Autorun Restore

Norton 360 Autorun Restore helps you restore the files that are backed up on an optical disc. You can also use this feature to restore your backed up files to a computer that does not have Norton 360 installed.

When you insert an optical disc that contains the backed-up files, the Autorun Restore feature automatically opens the **Portable Restore** window.

If you disable Windows auto-run option, you must manually launch the Autorun Restore feature.

The **Portable Restore** window provides you the following information:

- The name of the backup set
- The size of the backed-up files
- The date and time you backed up the files

You can select the files that you want to restore. You can restore the files to their original location. By default, Autorun restores the files you select to C:\Restored Files\. You can customize the location where you want to restore the selected files.

You can also launch the Norton 360 main window if Norton 360 version 3.0 or later is installed on your computer. If Norton 360 version 3.0 or later is not installed on your computer, Autorun tells you that the product is not installed on your computer.

You can also use the following link to obtain more information:

http://www.symantec.com/norton/360

Restoring files by using Norton 360 Autorun Restore

Norton 360 Autorun Restore lets you restore your files backed-up on an optical disk. Autorun can restore your backed-up files to a computer that does not have Norton 360 installed on it.

You can restore your backed-up files to their original locations or custom locations. You can also use the **Launch Norton 360** option in the **Portable Restore** window to open the Norton 360 main window. Norton 360 version 3.0 or later must be installed on your computer to open Norton 360.

To restore files using Norton 360 Autorun Restore

1. Insert an optical disc that contains the backed-up files.
2. Click the **ARestore** icon to launch the Autorun Restore feature.
   If the **Windows AutoPlay** option is disabled, navigate to the optical disk that has your backup, and double click the **ARestore** icon to launch the Autorun Restore feature.
3. In the **Portable Restore** window, click **Select Files to Restore** option.
4. In the window that appears, in the left pane, under **Category**, click a file category from which you want to restore files.
5. In the right pane, check the files that you want to restore.
   If you want to restore all the files, in the left pane, under **Category**, click **All file types**, and then check the check box in the header close to **Backup Item**.
6. Under **Restore to**, click one of the following:
   - **Original Location**
     Choose this option if you want to restore the files to the original location.
   - **Custom Location**
     Choose this option if you want to restore the files to a new location. By default, Autorun restores the files you select to C:\Restored Files\.
7. Click **Restore Selected**.
8. Follow the on-screen instructions to finish restoring your files.

About Norton Backup Drive

Norton 360 provides the Norton Backup Drive in your Windows Explorer after you configure your backup. Norton Backup Drive contains a list of backup destinations where your files are backed up. Each

backup destination contains the backup sets to which the backup destination is configured.

Norton Backup Drive displays the files that you backed up to a media device. You must connect and turn on the media device before you view your files.

You can also view the files that you backed up to Secure Online Storage. You must be connected to the Internet and logged in to Norton Account.

To view the files in your online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

The Norton Backup Drive is accessible only to system administrator.

You can do the following with Norton Backup Drive:

- View the files that are backed up in different backup destinations.

  To view the files that you backed up to a media device, you must connect the device to your computer.
- Restore a file from a backup set on the Norton Backup Drive to restore to your computer.
- Select and delete a file from a backup set on the Norton Backup Drive.

  Norton 360 does not back up the file you deleted the next time you run backup.
- Open a file to view the content of the file before you restore or delete it on the Norton Backup Drive.
- Use the **Search** command on the **Start** menu or the **Search Toolbar** option to locate files in the Norton Backup Drive.

Norton Backup Drive appears in Windows Explorer only when the **Backup** option in the **Backup Settings** window is turned on.

Viewing backup files on the Norton Backup Drive

You can use the Norton Backup Drive to view the files that are backed up. You can view the Norton Backup Drive after you configure backup.

If you backed up your files to a media device, ensure that the device is connected to your PC and turned on. You can then view the files on the Norton Backup Drive.

If you backed up your files to Secure Online Storage, you must be connected to the Internet. You must also be logged in to Norton Account to view the files on the Norton Backup Drive.

To view the files in your online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window

To view backup files on the Norton Backup Drive

1. In Windows Explorer, click **Norton Backup Drive**.
2. Select the backup destination, and navigate to the backup set that contains the files that you backed up.

Restoring a file from a backup set on the Norton Backup Drive

To restore a file, you can drag it from a backup set on the Norton Backup Drive to your computer. You can also click to open and view the contents of the file before you restore it.

Right-click to select the files to restore in the Norton Backup Drive, and then click **Restore to**. You can restore your backed-up files to their original locations or custom locations.

To restore a file from a backup set on the Norton Backup Drive

1. In Windows Explorer, click **Norton Backup Drive**.

2 Select the backup destination, and navigate to the backup set destination that contains the file that you backed up.
3 Do one of the following:
- Right-click to select the files to restore in Norton Backup Drive, and then click **Restore**.

  The files are restored to the original location by overwriting the existing files.
- Right-click to select the files to restore in the Norton Backup Drive, and then click **Restore to**.

  You can choose to restore your files to the **Original Location** or to a **New Location**.

4 Click **OK**.

Deleting a file from a backup set on the Norton Backup Drive

You can select and delete a file from a backup set on the Norton Backup Drive. Norton 360 does not back up the deleted file the next time you run a backup. You can also click the file to open and view the file content before you restore it.

To delete a file from a backup set on the Norton Backup Drive

1 In Windows Explorer, click **Norton Backup Drive**.
2 Select the backup destination, and navigate to the backup set destination that contains the file that you backed up.
3 Do one of the following:
- Right-click to select the files to delete, and then click **Delete**.
- Select the file, and then press **Delete**.

About solutions to the backup problems

The following table provides some tips to help you avoid backup problems.

All backups	The following tips apply to all backups: ▪ Perform backups regularly. The more often you back up, the less chance there is that you can lose important information. An automatic backup schedule is recommended, since that tends to back up those files that have most recently changed. A scheduled weekly backup is a good second choice. ▪ If you use automatic backups, leave your PC turned on when not in use. Automatic backups take place when your PC is turned on but not in use. ▪ Regularly check the backup results that Norton 360 provides to ensure that all of the files that should be backed up are backed up.

Backing up to CDs or DVDs	The following tips apply to backups to CDs or DVDs: ▪ Have extra discs on hand when you back up. This tip helps you to avoid occasional disc flaws or situations where the amount of backed up data is more than you anticipated. ▪ Label your backup discs with the complete details, so that you can find the right disc when you need to restore files. ▪ Do not copy files directly from the backup discs to your PC. You may inadvertently copy only part. Instead, use the Norton 360 restore feature or use the Norton 360 Autorun Restore feature.

Backing up to external drives, including flash drives	The following tips apply to backups to external drives: ▪ Some drives use older Windows file systems, such as FAT-16 or FAT-32 that cannot store files larger than 4 GB. For such large files to back up, ensure that your backup drive is formatted with a file system that supports large files, such as NTFS. ▪ If you use automatic or scheduled backups, make sure that the external drives are connected and turned on. ▪ To avoid accidentally corrupting your backed up files, do not use a backup drive for purposes other than for backing up.

Backing up to your Secure Online Storage	The following tips apply to backups to online storage: ▪ Make sure that your PC does not automatically disconnect from the Internet when it is not in use. ▪ Regularly check the amount of space that you have left in your Secure Online Storage, and consider purchasing more storage space before you need it. ▪ Online backups work best with a fast Internet connection. If your backups take too long, consider backing up only the files that you regularly work. Then periodically back up to CDs, DVDs, Blu-ray discs, or external drives to back up your larger, seldom-used files. ▪ If you back up more than one PC to your online storage, give each PC a different nickname. Giving a different nickname to each PC helps you identify the PC and the backups that corresponds to each PC.

Getting additional help with backup problems

If you run into problems with your Symantec product that you cannot solve, or have questions about the product, additional help is available. You can use the **Norton Autofix** window to open the support Web site

and search the Symantec Knowledge Base for solutions to your problem.

To get additional help with backup problems

1. In the Norton 360 main window, click **Support**, and then click **Get Support**.
2. In the **Norton Autofix** window, click **Open Support Web Site** to launch the support Web site.

About online backup considerations

Norton 360 provides you with secure backup storage space on a server that is accessible to your computer through its Internet connection. When your backup location is distant from your computer, your data is safe from local disasters, such as a fire, flood, or earthquake.

To use online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

Although online backup is convenient and safe, before choosing it for your backup method, consider the following limitations:

Speed limitations	

	The amount of time that it takes to transfer your backup to the Secure Online Storage depends on the speed of your Internet connection. If you have many files to back up, the first backup can take hours or days, depending on the speed of your Internet connection. You can configure the Internet bandwidth that backup uses to back up your files using the **Bandwidth Throttle** option. This option is available on the **Where** tab of the **Manage Backup Sets** window. You can alter the following bandwidth throttle states: ▪ **Fastest (recommended)** ▪ **High usage** ▪ **Moderate usage** ▪ **Low usage** Furthermore, many home and small business Internet connections are asymmetrical, meaning that their upload speeds are slower than their download speeds. A single large file, such as a high-quality photograph, may take several minutes or longer to upload to your Secure Online Storage. If you have many large files and asymmetrical or slow Internet connection, consider the use of one of the other backup locations that Norton 360 provides. You can then use your Secure Online Storage to back

	up your smaller files, such as your financial documents and word-processing documents. If a backup is in progress, you should leave your computer turned on, so that the backup can finish. However, if a backup is interrupted, then the next time it starts, it resumes where it left off and continues until it finishes.
Storage limitations	Norton 360 provides sufficient online storage to handle many of your backup needs, and you can purchase more storage when you need it. Nonetheless, the amount of space in your Secure Online Storage is much smaller than the typical permanent disk that most recent computers have. Online backups are ideal for the files that you regularly work on. You can back up large files and the files that seldom change to a different location. In addition, you should periodically look over the files that you have in your Secure Online Storage. Eliminate those files that you no longer need, to make additional storage space available.

About online backup activation

Norton 360 uses your Norton Account to keep track of the following:

- The computers that you back up to online storage

- The amount of online storage space that is available to you

Your product needs to be activated to use the online backup feature. The first time you configure online backup, Norton 360 connects to your Norton Account and requests that you sign in to the account. You may have established a Norton Account when you installed Norton 360 or when you installed another Norton product.

To sign in to your Norton Account, you use the email address and the password that you supplied when you created your Norton Account. You only need to sign in to your Norton Account the first time that you configure online backup. Norton 360 retains your account information so you do not have to sign in again. If you do not have a Norton Account when you configure online backup for the first time, Norton 360 lets you create one.

Symantec provides 2 GB of online storage for each Norton 360 product key. You can share the online storage space that is allocated to you using your Norton Account among your computers. For example, you have two computers having Norton 360 installed on it and registered with the same Norton Account. You can share the storage space among your two computers. You use 1 GB of online storage space for your first computer. When you activate the online storage for your second computer using the same Norton Account, that computer can use the remaining 1 GB of space.

To use online backup, you must configure the **Metered Broadband Mode** option in the **My Network** window to **No Limit**. The **My Network** option is available in the **Settings** window.

Purchasing more online storage space

Your Norton 360 subscription comes with an allotment of secure online storage space. When Norton 360 performs an online backup, it calculates the amount of space that it needs for the backup. If your online

storage does not contain sufficient space for the backup, Norton 360 notifies you and provides you an option to buy more space.

You do not have to wait until Norton 360 tells you that you need more online storage space. You can purchase additional space at any time.

You must be connected to the Internet to purchase more online storage space.

It can take about 30 seconds for the status on the **My Account** page to display the amount of space that you purchased.

To purchase additional online storage space when backing up

1. When Norton 360 notifies you that it needs more online storage space, click **Buy More Storage**. Your Web browser opens to a secure page, on which you can purchase additional online storage space.
2. Follow the instructions on the secure Web page to purchase additional online storage space.

To purchase additional online storage space at other times

1. In the Norton 360 main window, click **Backup**, and then click **Buy More Storage**. Your Web browser opens to a secure page, on which you can purchase additional online storage space.
2. Follow the instructions on the Web page to purchase additional online storage space.

Turning off or turning on backup

When the **Backup** option is turned on, Norton 360 automatically backs up your files when your computer is idle. However, if you want to temporarily disable backup, you can turn it off from within the program.

When you turn off backup, the backup status in the Norton 360 main window changes from **Protected** to **Disabled**. In the Disabled state, Norton 360 disables

all automatic backup of files. You can use the **Run Backup Now** option in the main window if you want to back up your files from all the backup sets.

You can turn off or turn on backup from the **Settings** window, **Backup Settings** window, or from the **Backup Details** window.

To turn off or turn on backup from the Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, do one of the following:
   - To turn off backup, uncheck **Backup**.
   - To turn on backup, check **Backup**.

To turn off or turn on backup from the Backup Settings window

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Backup Settings**.
3. In the **Backup Settings** window, do one of the following:
   - To turn off backup, move the **On/Off** switch to the right to the Off position.
   - To turn on backup, move the **On/Off** switch to the left to the On position.
4. In the **Settings** window, click **Apply**.

To turn off or turn on backup from the Backup Details window

1. In the Norton 360 main window, click **Backup**, and then click **View Details**.
2. In the **Backup Details** window, under **Things You Can Do**, do one of the following:
   - To turn off backup, click **Turn Off Backup**.
   - To turn on backup, click **Turn On Backup**.

Turning off or turning on backup setting options

Norton 360 provides you various options to manage your backup settings. Norton 360 backup settings let you access the backup details of a particular file by status icon overlays without opening the product. You can use the icon overlays to view the backup status of a file or folder. You can also use the **Properties** page of a file to know the backup status of your backup sets.

When the **Backup Status Overlays** option is turned on, Norton 360 adds a backup status icon to the files, based on the following conditions:

- The files belong to a backup file category that you included in any of the backup sets.
- The files are located at a source that you included in any of the backup sets.

The following table lists the backup status overlay icons for the files on your computer:

Green icon with a check mark	Indicates that the file has been backed up This icon changes to blue icon with arrows if you modify the file.
Blue icon with arrows	Indicates that the file has not been backed up This icon changes to green when Norton 360 automatically backs up the file during idle time.

Gray icon with a slash mark	Indicates that the file has been excluded from backup Norton 360 displays a disabled backup status on a file when you exclude the file from any of the backup sets.

Norton 360 Backup provides the Norton Backup Drive in your Windows Explorer after you configure your backup. Norton Backup Drive contains a list of backup destinations where your files are backed up.

You can use the **Context Menu** option to add or exclude a file or a folder to your backup sets when you right-click it. You can use this option after you configure Backup in the **Manage Backup Sets** window.

You can use the **Property Page** option to view more details about the backup status icons. When you right-click a file that you backed up and view the File Properties, you can see its backup details on the **Backup** tab. The **Backup** tab lists the state of the file for each backup set and the last backup time.

You can turn off these options if you do not want to see the icons and backup statuses.

To turn off backup setting options

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Backup Settings**.

3 In the **Backup Settings** window, do one of the following:

- To turn off icon overlays, in the **Backup Status Overlays** row, move the **On/Off** switch to the right to the Off position.
- To turn off **Norton Backup Drive**, in the **Norton Backup Drive** row, move the **On/Off** switch to the right to the Off position.
- To turn off right-click backup menu, in the **Context Menu** row, move the **On/Off** switch to the right to the Off position.
- To turn off **Backup** tab in the **Properties** page, in the **Property Page** row, move the **On/Off** switch to the right to the Off position.

4 In the **Settings** window, click **Apply**.

To turn on backup setting options

1 In the Norton 360 main window, click **Settings**.

2 In the **Settings** window, under **Detailed Settings**, click **Backup Settings**.

3 In the **Backup Settings** window, do one of the following:

- To turn on icon overlays, in the **Backup Status Overlays** row, move the **On/Off** switch to the left to the On position.
- To turn on **Norton Backup Drive**, in the **Norton Backup Drive** row, move the **On/Off** switch to the left to the On position.
- To turn on right-click backup menu, in the **Context Menu** row, move the **On/Off** switch to the left to the On position.
- To turn on **Backup** tab in the **Properties** page, in the **Property Page** row, move the **On/Off** switch to the left to the On position.

4 In the **Settings** window, click **Apply**.

Customizing settings

13

This chapter includes the following topics:

- About Norton 360 Settings
- Customizing Norton 360 Settings
- Turning on or turning off Quick Controls services
- About Antivirus settings
- About Firewall settings
- About Norton AntiSpam settings
- About My Network settings
- About backup settings
- About Identity Protection settings
- About Task Scheduling settings
- About Administrative Settings

About Norton 360 Settings

The **Detailed Settings** in the **Settings** window let you adjust protection settings and network settings. You can also customize schedules for security scans and backups.

You can configure the following **Detailed Settings** in the **Settings** window:

Antivirus	Specify how certain types of viruses and spyware, as well as other threats, are handled in Norton 360. You can specify whether incoming emails are checked and instant messenger is scanned. You can also specify which files and signatures are excluded from scans, and how low-risk threats are handled. In addition, you can configure Real Time Protection, Antispyware, and LiveUpdate.
Firewall	Specify in detail how to handle incoming and outgoing connections for your PC. You can specify Traffic rules and rules for specific programs. You can also specify how you want Norton 360 to handle intrusion attempts and browser protection.
AntiSpam	Secure your email client from unwanted online content. You can configure Norton AntiSpam to define which client it should integrate with and how it should handle the email that it scans on those clients. You can specify if you want Norton AntiSpam to check the Symantec servers to filter the spam email messages which the local filters classify as legitimate.

My Network	View all the devices available in your network and specify the trust level of the devices that are connected to your network. You can hide or show the **Network Security Overview** window at startup and configure the communication port that Norton products use to communicate with each other. You can also purge the Network Security Map.
Parental Controls	Lets you download and install Norton Safety Minder and configure Norton Online Family. Norton Online Family is a parental control application that provides a smart way to keep your children safe when they are online. Norton Safety Minder is an application that needs to be installed on each computer that your child uses to monitor the Internet activities. You can use the **Parental Controls** link to visit Norton Online Family Web page to download Norton Safety Minder. Click **Download Norton Safety Minder** to download Norton Safety Minder. Follow the on-screen instructions to complete the installation. If you have already installed Norton Safety Minder, you can click **Parental Control** to open the **Parental Control** settings window.

Identity Protection	Configure Identity Safe to secure your online identities and transaction data. You can also configure **Safe Surfing** options.
Tasks Scheduling	Specify when and how often Norton 360 examines your computer for viruses and other risks.
Administrative Settings	Use the options in this window to configure the security of your product. You can specify your proxy settings in Norton 360. You can also configure Idle Time Optimizer, Performance Monitoring, and Power Saving Mode. In addition, you can configure Silent Mode, Idle Time Out duration, Automatic Tasks Delay duration, Norton Community Watch, and Firefox Cleanup.
Backup Settings	Specify the files and folders that you want to back up, the backup location, and the backup schedule. You can also turn off or turn on options such as **Backup Status Overlays**, **Norton Backup Drive**, **Context Menu**, and **Property Page**.

The **Quick Controls** in the **Settings** window let you turn on or turn off the following services:

Silent Mode	Turns on or turns off Silent Mode You can turn on **Silent Mode** for a period of one hour, two hours, four hours, six hours, or one day.
Safe Surfing	Turns on or turns off Antiphishing and Norton Safe Web features When you turn on **Safe Surfing**, it protects your computer while you browse with Internet Explorer or Firefox.
Identity Safe	Turns on or turns off Identity Safe When you turn off Identity Safe, Norton 360 no longer lets you manage your logins, cards, and notes.
Backup	Turns on or turns off Backup When you turn on Backup, your computer starts backing up with your specified settings.
Backup Status Overlays	Turns on or turns off icon overlays on files Icon overlays show the backup status of your files.
Automatic LiveUpdate	Turns on or turns off the automatic updates that guard against new and emerging threats

Smart Firewall	Turns on or turns off Smart Firewall When you turn on Smart Firewall, it monitors communications between your computer and the other computers on the Internet. It also protects your computer from common security problems.
Norton Tamper Protection	Turns on or turns off Norton Tamper Protection When you turn on Norton Tamper Protection, it protects Norton 360 from attacks or modifications by unknown, suspicious, or threatening applications.

Customizing Norton 360 Settings

The default Norton 360 settings provide a safe, automatic, and efficient way to protect your computer. However, if you want to change or customize your protection settings, you can access most features from the Settings window.

You can configure Norton 360 settings in the following ways:

- You can use the **On/Off** switch to turn on or turn off a feature. When you turn off a feature, the color of the **On/Off** switch turns red, which indicates that your computer is vulnerable to security threats. When you turn on a feature, the color of the **On/Off** switch turns green, which indicates that your computer is protected against security threats.
- You can drag the slider of a protection feature to your preferred setting. Most often, Norton 360

provides the slider setting for you to decide whether to resolve security threats automatically or ask you before it takes an action.

- You can configure a protection feature by either selecting the options that are provided for the configuration or by providing the required information. Most of these options are available as check boxes for you to check or uncheck.

  You can also use the **Default All** option to reset the configuration to the default level.
- You can select a preferred option from the drop-down list.
- You can check or uncheck the **Quick Controls** options to turn on or turn off a feature.

Norton 360 also provides the **Use Defaults** option in most of the **Settings** window. You can use this option to reset the configuration to the default level.

To customize Norton 360 settings

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, click the protection feature that you want to customize.
3. In the window that appears, set the option to your preferred settings.
   You may need to click a tab to access the settings that are listed under that tab.
4. In the **Settings** window, do one of the following:
   - To save the changes, click **Apply**.
   - To close the window without saving the changes, click **Close**.

Turning on or turning off Quick Controls services

In the **Settings** window, you can turn on or turn off the following **Quick Controls** services:

- **Silent Mode**

- **Safe Surfing**
- **Identity Safe**
- **Backup**
- **Backup Status Overlays**
- **Automatic LiveUpdate**
- **Smart Firewall**
- **Norton Tamper Protection**

You can move the mouse pointer over a service name to see a description of that service. You should leave all of the services turned on except Silent Mode.

To turn on or turn off Quick Controls services

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Quick Controls**, do one of the following:
   - To turn on a service, check its check box.
   - To turn off a service, uncheck its check box.

     If an alert or a message appears, select the duration from the drop-down menu, and then click **OK**.

About Antivirus settings

Norton 360 always protects you from known viruses and the latest virus outbreak. The Antivirus settings monitor your PC for the presence of viruses and spyware, as well as other threats, and either quarantines or remove them.

The Antivirus settings protect your computer against the security risks that can compromise your personal information and privacy. The different type of scans, such as Computer Scans, Email Antivirus Scan, and Instant Messenger scan detects and prevents from any virus infection on your computer.

The Antivirus settings obtain the latest virus definitions through definition updates and keep your computer secure from the latest security threats.

You can use the following Antivirus settings:

Automatic Protection	The Automatic Protection settings let you control the scanning and monitoring of your computer. It protects your computer by continuously checking for viruses and other security risks. Your options are: ▪ **Real Time Protection** You can use the **Real Time Protection** options to protect your computer by continuously checking for viruses and other security risks. ▪ **Boot Time Protection** You can use the **Boot Time Protection** option to provide an enhanced security level from the time you start your computer. This option ensures better security by running all the necessary components that are required for computer protection as soon as you restart your computer.

Scans and Risks	

Scans and Risks settings let you customize the scans that Norton 360 performs on your computer.

You can use the following Scans and Risks options:

- **Computer Scans**

  Norton 360 lets you run different types of scans to detect and prevent any virus infection on your computer.

  You can use the various Computer Scans options to customize the scans that Norton 360 performs on your computer. You can also specify scanning of compressed files and Microsoft Office documents.
- **Scan Performance Profiles**

  Scan Performance Profiles settings let you configure how Norton 360 should scan your computer based on the digital signature and trust level of the files.
- **Protected Ports**

  Norton 360 protects the POP3 and SMTP ports of your email program.

  You can use this option to manually configure your POP3 and SMTP email ports for email protection. If the SMTP and POP3 port numbers that your Internet service provider (ISP) has provided for your email program is different from the default SMTP and POP3 port numbers, you must configure

	Norton 360 to protect the ports. ▪ **Email Antivirus Scan** Email Antivirus Scan protects you from the threats that are sent or received in email attachments. This option lets you define how Norton 360 should behave when it scans email messages. Based on the options you choose, Norton 360 automatically scans the email messages that you send or receive. ▪ **Instant Messenger Scan** The Instant Messenger Scan option lets you customize scanning of the files that you receive from instant messenger programs. You can select the supported instant messenger programs from which you may receive files. Norton 360 scans the files that you receive from the selected instant messenger programs.

- **Exclusions / Low Risks**

  Exclusions options specify the items such as folders, files, and drives that you exclude from Norton 360 scans. Scans, signatures, and low-risk items are some items that you can exclude from scanning

  Exclusions options let you choose which categories of risks you want Norton 360 to detect.

  Exclusions reduce your level of protection and should be used only if you have a specific need.

- **Insight Protection**

  The Insight Network scan uses the Cloud technology wherein a remote server on the web contains the latest virus definitions. Norton 360 scans your computer for the latest security threats. When Norton 360 performs the Insight Network scan, it uses the virus definitions that are available locally and in the Cloud. Norton 360 provides additional protection by using the most recent definitions in the Cloud, apart from the definitions that are available locally on your computer.

Antispyware and Updates	Antispyware protects your computer against the security risks that can compromise your personal information and privacy. Norton 360 protects your computer from vulnerabilities through the latest definition and protection updates. Your options are: **Antispyware** Antispyware protects your computer against the security risks that can compromise your personal information and privacy This option lets you choose which categories of risk you want Norton 360 to detect for manual, email, and instant messenger scanning. **Updates** Norton 360 protects your computer from vulnerabilities through the latest definition and protection updates. Definition updates contain the information that lets Norton 360 to recognize and alert you to the presence of a specific virus or security threat You can use the Updates options to obtain the latest virus definitions through definition updates and keep your computer secure from the latest security threats.

About Automatic Protection settings

The **Boot Time Protection** option on the **Automatic Protection** tab provides an enhanced security level from the time you start your computer. This option ensures better security by running all the necessary components that are required for computer protection as soon as you start your computer.

The **Real Time Protection** settings on the **Automatic Protection** tab let you control the scanning and monitoring of your computer. It protects your computer by continuously checking for viruses and other security risks.

You can use the **Real Time Protection** options to determine what gets scanned and what the scan looks for. It also provides you with advanced protection by proactively detecting unknown security risks on your computer. You can determine what happens when a security risk or risk-like activity is encountered.

You can use the following **Real Time Protection** options:

Auto-Protect	

Auto-Protect loads into memory and provides constant protection while you work. It checks for viruses and other security risks every time that you run programs on your computer.

Auto-Protect checks for viruses when you insert any removable media, access the Internet, or use the document files that you receive or create. It also monitors your computer for any unusual symptoms that might indicate an active threat.

You can stay protected by using the following options:

- **Caching**

  Improves the performance of your computer

  If you turn on this option, Norton 360 keeps a record of the files that are accessed often. Norton 360 does not scan those recorded files, even when you restart your computer.

- **Removable Media Scan**

  Checks for boot viruses when you access removable media

  After the removable media has been scanned for boot viruses, it is not scanned again until it is reinserted or formatted. If you still suspect that a

	boot virus infects your removable media, ensure that Auto-Protect is turned on to rescan the removable media. You then insert the removable media and open it from My Computer for Auto-Protect to rescan it. You can also scan it manually to verify that it is not infected.

SONAR Protection	

Symantec Online Network for Advanced Response (SONAR) provides the real-time protection against threats and proactively detects unknown security risks on your computer.

SONAR identifies the emerging threats that are based on the behavior of applications. SONAR is quicker than the traditional signature-based threat detection techniques. It also detects and protects your computer against malicious code even before virus definitions are available through LiveUpdate.

SONAR Protection includes the following options:

- **SONAR Advanced Mode**

  Norton 360 provides you the greatest control over low-certainty threats only if this option is turned on.
- **Remove Risks Automatically**

  This option lets the low-certainty threats behave as high-certainty threats when **SONAR Advanced Mode** option is enabled. In this case, Norton 360 automatically removes the threats and notifies you.
- **Remove Risks if I Am Away**

  This option lets Norton

	360 to automatically remove low-certainty threats if it does not get any response from you when **SONAR Advanced Mode** option is enabled. **Show SONAR Block Notifications** This option lets you enable or disable SONAR Block notifications. Norton 360 suppresses the SONAR Block notifications when you set the **Show SONAR Block Notifications** option to Log Only.

About Scans and Risks settings

Scans and Risks settings let you customize the scans that Norton 360 performs on your computer. You can configure a Norton 360 scan based on the digital signature and trust level of the files on your computer. You can define how Norton 360 should behave when it scans email messages and customize scanning of the files that you receive from instant messenger programs.

You can use the following Scans and Risks settings:

Computer Scans	

Norton 360 lets you run different types of scans to detect and prevent any virus infection on your computer. The scans are Quick Scan, Full System Scan, and Customized Scan. You can use the various Computer Scans options to customize the scans that Norton 360 performs on your computer. You can also specify scanning of compressed files and Microsoft Office documents.

The Computer Scans options also let you specify scans to detect rootkits, other stealth items, tracking cookies, and unknown security threats. Your options are:

- **Smart Definitions**

  Lets you install only the Core Set virus definitions.

  You can choose Smart Definitions to minimize download time, installation time, and memory consumption as Smart Definitions are a subset of virus definitions.
- **Compressed File Scan**

  Scans and repairs the files inside compressed files.

  When you turn on this feature, Norton 360 scans and detects viruses and other security risks in the files within compressed files and removes the compressed files.
- **Microsoft Office Automatic Scan**

Scans the Microsoft Office files when you open them.

If you install Microsoft Office 2000 or later after Norton 360 is installed, you must turn on this option to scan Microsoft Office files automatically.

- **Rootkits and Stealth Items Scan**

  Scans for rootkits and other security risks that might be hidden on your computer.

- **Network Drives Scan**

  Scans the network drives that are connected to your computer.

  Norton 360 performs a **Network Drives Scan** during **Full System Scan** and **Custom Scan**. By default, the **Network Drives Scan** option is turned on. If you turn off this option, Norton 360 does not scan network drives.

- **Heuristic Protection**

  Scans your computer to protect against unknown security threats.

  Norton 360 uses heuristic technology to check suspicious characteristics of a file to categorize it as infected. It compares the characteristics of a file to a known infected file. If the file has sufficient suspicious characteristics, then Norton 360 identifies the file as infected with a threat.

	▪ **Tracking Cookies Scan** Scans for the small files that programs might place on your computer to track your computing activities. ▪ **Full System Scan** Scans your computer when it is idle. When your computer is idle, Norton 360 runs a Full System Scan. After the scan is complete, you can view the summary of the scan results and take appropriate action when you start using your computer again. You can use the **Configure** option to schedule the Full System Scan. ▪ **Number of Threads for Manual Scan** Lets you select the number of threads that Norton 360 uses for manual scan Threads are subsets of a process that share the process resources but execute independently of each other. Threads help in parallel execution of a program to allow the program to operate faster in a multiprocessor environment.

Scan Performance Profiles	The Scan Performance Profiles settings let you configure how Norton 360 should scan your computer based on the digital signature and trust level of the files. You must configure the Scan Performance Profiles settings before you run a scan or before a scan is scheduled to run. Norton 360 scans your computer according to the configuration you specified in the Scan Performance Profiles settings. You can configure the following Scan Performance Profiles settings: **Full Scan** Configure a complete scan of your computer. **Standard Trust** Configure a scan that excludes the files that are Norton Trusted. **High Trust** Configure a scan that excludes the Norton and Community Trusted files and the files that have known digital signatures.

Protected Ports	Protected Ports settings protect the POP3 and SMTP ports of your email program. You can use this option to manually configure your POP3 and SMTP email ports for email protection. If the SMTP and POP3 port numbers that your Internet service provider (ISP) has provided for your email program is different from the default SMTP and POP3 port numbers, you must configure Norton 360 to protect the ports.
Email Antivirus Scan	Email Antivirus Scan protects you from the threats that are sent or received in email attachments. You can use the Email Antivirus Scan options to define how Norton 360 should behave when it scans email messages. Based on the options you choose, Norton 360 automatically scans the email messages that you send or receive.
Instant Messenger Scan	Instant Messenger Scan options let you customize the scanning of the files that you receive from instant messenger programs. You can select the supported instant messenger programs from which you may receive files. Norton 360 scans the files that you receive from the selected instant messenger programs.

Exclusion / Low Risks	

Exclusions options specify the items such as folders, files, and drives that you exclude from Norton 360 scans. Scans, signatures, and low-risk items are some items that you can exclude from scanning.

Exclusions options also let you choose which categories of risks you want Norton 360 to detect. Your options are:

- **Low Risks**

  Lets you manage the low-risk items that are found in your computer.

  You can specify how you want Norton 360 to respond to low-risk items.
- **Items to Exclude from Scans**

  Lets you determine which disks, folders, or files you want to exclude from risk scanning.

  You can add new exclusion items or edit the added items in the excluded-items list. You can also remove items from the excluded-items list.
- **Items to Exclude from Auto-Protect and SONAR Detection**

  Lets you determine which disks, folders, or files you want to exclude from Auto-Protect scans and SONAR scans.

  You can add the new items that need to be excluded or modify the items that you already excluded. You can

	also remove items from the excluded-items list. **Signatures to Exclude from All Detections** Lets you select known risks by name and remove a risk name from the excluded-items list You can also view the risk impact that is based on the performance, privacy, removal, and stealth impact. Exclusions reduce your level of protection and should be used only if you have a specific need.
Insight Protection	The Insight Network scan uses the Cloud technology wherein a remote server on the Web contains the latest virus definitions. Norton 360 scans your computer for the latest security threats. When Norton 360 performs the Insight Network scan, it uses the virus definitions that are available locally and in the Cloud. Norton 360 provides additional protection by using the most recent definitions in the Cloud, apart from the definitions that are available locally on your computer.

About Antispyware and Updates settings

Antispyware protects your computer against the security risks that can compromise your personal information and privacy.

Security risks, such as spyware and adware, can compromise your personal information and privacy. Spyware and adware programs are closely related. In some cases, their functionalities may overlap; but while they both collect information about you, the types of information that they collect can differ.

Norton 360 protects your computer from vulnerabilities through the latest program updates and definition updates. Automatic LiveUpdate and Pulse Updates obtain the latest virus definitions through definition updates and keep your computer secure from the latest security threats.

You can use the following Antispyware and Updates settings:

Antispyware	Antispyware options let you choose which categories of risk you want Norton 360 to detect for Auto-Protect, manual, email, and instant messenger scans.

Updates	Norton 360 protects your computer from vulnerabilities through the latest program and definition updates. Definition updates contain the information that lets Norton 360 recognize and alert you to the presence of a specific virus or security threat. You can use the Updates options to obtain the latest virus definitions through definition updates and keep your computer secure from the latest security threats. Your options are: **Automatic LiveUpdate** Automatic LiveUpdate automatically checks for definition and program updates when you are connected to the Internet. **Pulse Updates** In addition to the definition updates that Automatic LiveUpdate downloads, Norton 360 uses streaming technology to download the latest virus definitions. These downloads are called Pulse Updates. The Pulse Updates are lighter and faster, and keep your computer secure from the ongoing threats on the Internet.

About Firewall settings

Firewall settings in Norton 360 check your PC's Internet connection to protect it from unwanted communication activity and Internet intrusions.

The following tabs are available in the **Firewall** settings window:

General Settings	Lets you activate the general firewall features and customize the ports that your computer uses to access Web pages The general settings let you control how firewall handles the uncommon protocols and the network traffic to and from your computer. According to the general settings, the firewall allows or blocks the incoming or the outgoing connection attempts and the sharing of resources with your computer. You can also use the general settings to let the firewall control connection attempts to or from the blocked and the inactive ports in your computer.
Program Rules	Lets you control settings for the programs that access the Internet
Traffic Rules	Lets you determine how the firewall handles incoming and outgoing network connections of various kinds You can change the settings to allow or deny specific types of connections with your PC.

Intrusion and Browser Protection	Prevents intrusion attempts and protects your Web browser from attacks by malicious Web sites You can use the **Download Intelligence** option that is available on this tab to protect your computer against any unsafe file that you download. This feature supports only downloads using the HTTP protocol and Internet Explorer and Firefox browsers.

Advanced Settings	Lets you activate the advanced protection features of Smart Firewall The advanced settings let you turn on or turn off the Automatic Program Control feature. Automatic Program Control automatically configures Internet access settings for the Web-enabled programs that you run for the first time. The **Automatic Learn IPv6 NAT Traversal Traffic** option is available only when Automatic Program Control is turned on. Norton 360 provides the Automatic Learn IPv6 NAT Traversal Traffic option to control the network traffic that uses Teredo to communicate with your computer. When you turn off Automatic Program control, you can turn on Advanced Events Monitoring. You can use the **Advanced Events Monitoring** options to configure the Internet access settings for Internet-enabled programs the first time that they run.

About Firewall General settings

Smart Firewall General settings let you activate the general firewall features and customize the ports that

your computer uses to access Web pages. Your options are:

Uncommon Protocols	Determines how the Smart Firewall handles uncommon protocols.
Firewall Reset	Returns the Smart Firewall to its default state. You can use the **Reset** option to ensure that all recommended firewall rules and settings are configured. If you reset the firewall, you remove any custom rules or settings that you have configured. Therefore, Norton 360 prompts you with a confirmation dialog box when you reset firewall.
Stealth Blocked Ports	Ensures that blocked and inactive ports do not respond to connection attempts. Active ports are prevented from responding to connection attempts that have incorrect source or destination information.

Stateful Protocol Filter	Automatically allows the Internet traffic that matches the connections that an application opens. Check this option to do the following: ▪ Analyze the network traffic that enters your computer. ▪ Block the suspicious applications that try to connect to your computer.
Automatic File/Printer Sharing Control	Allows the computers on the network to share resources such as files, folders, and printers (that are locally attached).
Block All Network Traffic	Blocks all network communications to and from your computer.

About the Intrusion and Browser Protection settings

Intrusion Prevention scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects your computer against most common Internet attacks.

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects your computer from being affected in any way.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. Norton 360 runs LiveUpdate automatically to keep your list of attack signatures up

to date. If you do not use Automatic LiveUpdate, you should run LiveUpdate once a week.

Norton 360 also provides the Web Browser Protection feature to protect your Web browser from malicious programs.

The Browser Protection feature is available for Internet Explorer 6.0 or later, Chrome 10.0 or later, and Firefox 3.6 or later.

With increasing Internet use, your Web browser is prone to attack by malicious Web sites. These Web sites detect and exploit the vulnerability of your Web browser to download malware programs to your system without your consent or knowledge. These malware programs are also called drive-by downloads. Norton 360 protects your Web browser against drive-by downloads from malicious Web sites.

The **Intrusion and Browser Protection** settings also include the **Download Intelligence** option to protect your computer against any unsafe file that you download. Download Intelligence provides information about the reputation level of any executable file that you download using the Web browser. Download Intelligence supports only downloads using the HTTP protocol, Internet Explorer 6 browser or later, Chrome 10.0 browser or later, and Firefox 3.6 browser or later. The reputation details that Download Intelligence provides indicate whether the downloaded file is safe to install. You can use these details to decide whether you want to install the executable file.

About Smart Firewall Advanced settings

Smart Firewall Advanced settings let you activate the advanced protection features of Smart Firewall by turning off Automatic Program Control.

Automatic Program Control automatically configures Internet access settings for the Web-enabled programs that are run for the first time. The **Automatic Learn IPv6 NAT Traversal Traffic** option is available only

when Automatic Program Control is turned on. You can use this option to specify how Norton 360 must control any network traffic that uses Teredo to communicate with your computer.

When you turn off Automatic Program control, you can turn on Advanced Events Monitoring. You can use the **Advanced Events Monitoring** options, to configure the Internet access settings for Internet-enabled programs the first time that they run. When you turn on the Advanced Events Monitoring feature, you are prompted with numerous firewall alerts. You can allow or deny any of the events that may harm your computer. When the event occurs for the first time, a firewall alert appears and you can allow or block the event. When you allow the event, the event details appear under the relevant category that is available in Advanced Events Monitoring. The application that triggers the allowed event is added to the Trusted list of its corresponding category in Advanced Events Monitoring. You can remove the application from the list. In this case, firewall alert appears when the application triggers the event next time.

The Advanced Events Monitoring settings consist of the following categories that provides your computer with advanced protection:

Program Component	Monitors the malicious programs that launch Internet-enabled programs.
Program Launch	Monitors the malicious programs that attach to safe programs without being detected.
Command Line Execution	Monitors the Trojan horses or malicious programs that launch trusted applications in hidden mode through command-line parameters.

Code Injection	Monitors the Trojan horses or malicious programs that inject code into an application's process without triggering firewall alerts.
Window Messages	Monitors the Trojan horses and other malicious programs that manipulate an application's behavior to connect to the Internet without triggering firewall alerts.
Direct Network Access	Monitors the Trojan horses and other malicious programs that bypass network traffic. These programs penetrate the Windows TCP/IP layer to send and receive data without triggering firewall alerts.
Active Desktop Change	Monitors the malicious programs that use the documented interfaces that the trusted applications provide to transmit data outside the network without triggering firewall alerts
Key Logger Monitor	Monitors the malicious keylogger programs that access personal information of a user on a particular computer by monitoring their keystroke activities.
COM Control	Monitors the malicious programs that manipulate an application's behavior by instantiating controlled COM objects.

About Norton AntiSpam settings

With the increase in usage of email, many users receive a number of unwanted and unsolicited commercial email messages that are known as spam. Not only does spam make it difficult to identify valid email messages, but some spam contains offensive messages and images.

Norton AntiSpam incorporates several powerful features to reduce your exposure to unwanted online content.

Norton AntiSpam settings help you configure the following:

- The email client with which Norton AntiSpam should integrate
- The list of allowed email senders
- The list of blocked email senders
- The email addresses and domains that Norton AntiSpam should not import into the list of allowed and blocked email senders
- The option to send feedback to Symantec about misclassified email
- The option to filter email messages through Web Query to maintain high spam detection efficiency

You can configure Norton AntiSpam settings on the following tabs:

Filter	The options on the **Filter** tab let you configure the list of allowed and blocked email senders. You can also configure the option to filter the email messages through the Web Query filter. You can define whether feedback about a misclassified email message should be sent to Symantec. In addition, you can configure the **Address Book Exclusions** list.
Client Integration	The options on the **Client Integration** tab let you integrate Norton AntiSpam with your email clients to keep you free from unsolicited email messages. You can also specify whether or not to display a brief introduction of Norton AntiSpam each time you start your email program. In addition, you can specify which address book you want Norton AntiSpam to integrate with.

About Filter settings

The **Filter** tab in the **AntiSpam** settings window provides options to configure AntiSpam settings.

You can use the following options on the **Filter** tab:

Address Book Exclusions	Lets you exclude the email addresses that must not be automatically added from your address book to the Allowed List.

Allowed List	Lets you add specific addresses and domains (for example, @symantec.com) from which you want to receive email messages.
Blocked List	Lets you add specific addresses and domains from which you do not want to receive email messages. Norton AntiSpam marks all email messages from these addresses or domains as spam.
Web Query	Lets you check the Symantec Web servers to filter the spam email messages which the local filters classify as legitimate.
Protected Ports	Lets you configure your POP3 and SMTP email ports for email protection.

About Client Integration settings

The **Client Integration** tab in the **AntiSpam** settings window lists the supported email programs, or clients, that are installed on your computer and their associated address books.

You have the following options on the **Client Integration** tab:

Email Clients	Norton 360 supports Norton AntiSpam integration with Microsoft Outlook and Outlook Express. In Windows Vista, Norton 360 also supports Norton AntiSpam integration with Windows Mail. When you turn on an email client, Norton AntiSpam integrates with the email client.
Address Books	Norton 360 supports Norton AntiSpam integration with the address books of email clients from which you want Norton AntiSpam to import email addresses. You can also import into the Allowed List the list of addresses that are present in an email program. You do not have to integrate Norton AntiSpam with your email clients to import the addresses into the Allowed List.

The **Feedback** option under the **Miscellaneous** row lets you send feedback about the misclassified email message to Symantec.

The option is available only when Microsoft Outlook or Outlook Express is installed on your computer.

The **Welcome Screen** option under the **Miscellaneous** row provides a brief introduction of Norton AntiSpam each time you start your email program. You can turn off the **Welcome Screen** option if you do not want the welcome screen to appear.

The following email clients do not support client integration:

- Outlook 2010 64-bit
- Thunderbird
- Windows Mail

About My Network settings

The Network Security Map settings let you configure the communication port that Norton products use to communicate with each other. You can also specify whether to display the Network Security Overview window when you open Network Security Map.

You can use the **Configure** option in the **Network Security Map** row to access **Network Security Map** window. The **Network Security Map** window provides a pictorial representation of the devices on the network to which your computer is connected. You can view the details of each device before you set up Remote Monitoring. The **Product Configuration** panel appears when you click the **Configure** option for the first time. The **Product Configuration** panel helps you install the component that is required to view Network Security Map.

You have the following options:

Trust Control	Manages the trust level of the devices that you manually add to your home network. Trust Control is a special network that lists all the devices that you manually add to the Network Security Map, irrespective of their connection status. You can select the Trust Control network in the **Network Details** drop-down list to view the devices that you added. You can also reclassify the devices that you added to the Network Security Map as trusted or restricted. You cannot edit the details of Trust Control network.
Network Map	Removes all of the devices that are listed in Network Map. You can purge Network Map if you want to create a new list of devices. For example, you can purge all of the devices that were present on your previous network before you connect to a new network. Ensure that you disable Remote Monitoring before you purge the Network Map. Norton 360 cannot purge the Network Map when the Remote Monitoring is turned on. Norton 360 purges the devices that you add manually in the Trust Control network depending upon their trust level. It does not purge the devices that have a trust level of Full Trust or Restricted.

Communications Port	Shows the communication port that Norton products use to communicate with each other over the network. If you change the communication port number on your computer, you must change it on each computer that is connected to your Network Security Map. In addition, when you find more computers that use the Remote Monitoring Setup process, ensure that the same port number is used on every computer. Though this communication port is configurable, Symantec recommends that you do not change the port number to avoid potential conflicts with other well-known networking ports. If you change the communication port number, you must use a port number in the range 1-65535.
Welcome Screen at Startup	Displays the Network Security Overview window when you open Network Security Map.

About backup settings

You can use the backup settings in Norton 360 to configure your system backup.

Norton 360 Backup lets you perform the following tasks:

- Select the files that are required to be backed up.
- Choose the location to store the backed up files.
- Assign a schedule to run a backup.

In addition to the backup tasks, Norton 360 backup settings let you easily access the backup status of a

particular file without opening the product. The **Backup Settings** window provides you the option to turn off or turn on the Backup.

Under **Backup**, you have the following options:

Manage Backup	Lets you configure what, where, and when to back up your important files You can use the **Configure** option to specify the source, destination, and schedule of the backup.
Backup Status Overlays	Lets you view the backup status of a file by adding the status overlay to the file's icon The status overlays that appears are: ▪ Green icon with a check mark Indicates that the file has been backed up This icon changes to blue icon with arrows if you modify the file. ▪ Blue icon with arrows Indicates that the file has not been backed up This icon changes to green when Norton 360 automatically backs up the file during idle time. ▪ Gray icon with a slash mark Indicates that the file has been excluded from backup Norton 360 displays a disabled backup status on a file when you exclude the file from any of the backup sets.

Norton Backup Drive	Lets you view the list of backup destinations where your files are backed up in the Windows Explorer You can also add a file to a backup set and delete a file from a backup set. In addition, you can restore a file from a backup set on the Norton Backup Drive to your customized location.
Context Menu	Lets you add or exclude a file or a folder to a backup set by using the right-click shortcut menu You can use this option after you configure Backup in the **Manage Backup Sets** window. It lists down all the available backup sets for easy backups.
Property Page	Lets you view the backup status of each backup set on the **Backup** tab in the file Properties page that you included in your backup It lists down all the available backup sets along with the date and time that it was last backed up. It also shows the corresponding icon overlay that indicates if the file is included or excluded in a particular backup set.

Reserved Free Disk Space During Online Backup (in MB)	Lets you specify the amount of local disk space that you want to reserve. When you perform an online backup, Norton 360 creates a temporary file in your local disk for file transfer. At times, this file becomes large and consumes a large amount of free space available on your local drive. When the available free disk space on your computer reaches the specified limit, Norton 360 notifies you and does not perform an online backup. You must free some disk space and then perform an online backup. By default, Norton 360 reserves 2048 MB (2 GB) of your local disk space.

About Identity Protection settings

Identity thieves often use fraudulent Web sites to attempt to trick you into divulging private information. These sites may be disguised as shopping sites or financial transaction sites. Norton 360 helps guard against identity theft by verifying the Web sites you visit.

Antiphishing, Norton Safe Web, and Identity Safe features in Norton 360 let you safely browse the Internet and securely perform online transactions.

When you install Norton 360, it adds the **Norton Toolbar** to Internet Explorer, Chrome and Firefox. Norton 360 protects your Internet Explorer browser, Chrome browser, and Firefox browser when you turn on the **Safe Surfing** option.

Antiphishing tells you the following things about the Web pages that you visit:

- If it is safe to enter confidential information
- If the Web page is known to be fraudulent
- If the Web page is approved by Symantec
- If the Web page is known to belong to a suspicious site
- If the Web page is known to give annoying results

Norton Safe Web lets you know that a Web site is malicious before you visit it. It provides you a safe Web search environment by displaying the site rating icons next to every search result.

When you turn on Norton Safe Web, you can see the following site rating icons next to the search results:

Norton Secured icon	Indicates the site is VeriSign trusted
Green OK	Indicates that the site is safe to visit
Red cross (x) mark	Indicates that the site may attempt to install malicious software in your computer and is unsafe to visit
Yellow exclamation mark	Indicates that the site may provide annoying results
Grey question mark	Indicates that Norton Safe Web has not analyzed the site and it does not have sufficient information

The Identity Safe feature in Norton 360 lets you save and protect your logins. However, the feature remains inactive until you create an Identity Safe password and

log in to Identity Safe. The password protects you by restricting unauthorized access to your data in Identity Safe.

The Identity Safe feature provides you the ease of using your Identity Safe data when you are on the move. You can create an online vault and save your data in the online vault. You access your sensitive Identity Safe data from any computer that is connected to the Internet.

You can set up Identity Safe in the following areas of Norton 360:

- The **Identity Safe** section under **Identity Protection** option in the **Settings** window
- The **Identity Protection** section in the Norton 360 main window

Identity Safe provides you the following features for a secure online transaction experience:

Table 13-1 Identity Safe features

Feature	Description	Advice
Edit Logins	Lets you manage your login information This information includes such things as your email login credentials and Internet banking credentials.	When you save all of your login information in Identity Safe, you can do the following: - Easily track all of your logins - Quickly launch your login Web pages

Feature	Description	Advice
Edit Cards	Lets you manage your personal information in one place	You can use the information that you store in the cards to do the following: ▪ Automatically fill forms ▪ Provide sensitive information without having to type it while you are online In this way, Identity Safe protects you from keyloggers that steal and misuse your identity.

Feature	Description	Advice
Edit Notes	Lets you store and manage sensitive information In Edit Notes, you can include information such as Social Security number, driver license number, insurance policy number, and legal and financial information.	It becomes difficult to manage various identity numbers. Edit Notes stores all of your sensitive IDs in a very secure way and lets you easily use them while you are online.

About Task Scheduling settings

The Task Scheduling settings let you specify the tasks that Norton 360 should run automatically when your computer is idle. They also help you to schedule your activities that are related to security, performance, and backup.

Task Scheduling includes the following settings:

Automatic Tasks	Lets you specify the tasks that should run in the background automatically when your computer is idle These automatic tasks include activities that are related to PC Security and PC Tuneup. Your options are: **Internet Explorer Temporary Files** **Windows Temporary Files** **Internet Explorer History** **Disk Optimization** **Registry Cleanup**

Scheduling	

	Lets you schedule PC Security and PC Tuneup related activities You can specify how often Norton 360 should scan your system for security and performance issues and when it should perform backups. You have the following options for scheduling custom PC Security and PC Tuneup activities: **Automatic (Recommended)** This option is the recommended option. Norton 360 detects the time your PC is idle and then automatically runs the tasks. **Weekly** You can schedule to run your tasks on a weekly basis. You must specify the day and time. You can also specify that the schedule must run only when the PC is idle. **Monthly** You can schedule to run your tasks on a monthly basis. You must specify the time and the day of the month. You can also specify that the schedule must run only when the PC is idle. **Manual Schedule** You can run the tasks manually. Your computer's performance is maximized if you schedule your critical operations to occur when your computer is idle. Norton 360 identifies your computer as

	idle when there is no detectable mouse or keyboard activity for a period that you specify as idle timeout duration. When you schedule your scans weekly or monthly and check the **Run only at idle time** option, Norton 360 scans your computer when it is idle. Symantec recommends you to check the **Run only at idle time** option to experience better performance of your computer. You can use the **Click here to schedule backup** option to navigate to the **Manage Backup Sets** window. You can schedule your backup set in the **When** tab.

About Administrative Settings

You can use **Administrative Settings** window to configure various important options of Norton 360.

You have the following options:

Idle Time Optimizer	Lets you configure Norton 360 to defragment your boot volume or the local disk that contains the boot volume when your computer is idle. When the option is turned on, Norton 360 automatically schedules the optimization after you install an application on your computer. Optimization speeds up your computer's performance by defragmenting the fragmented parts of the disk.

Monthly Report	Lets you view how Norton 360 has protected you for the past 30 days. This report includes the activities that Norton 360 performed to protect your computer. You can turn on the **Monthly Report** option to let Norton 360 automatically display the Monthly Report once in every 30 days.
Automatic Download of New Version	Lets you automatically download the latest version of the Norton 360. You can easily upgrade to the latest version of Norton 360 when prompted. By default, this option is turned on. Symantec recommends you to install the latest product version as it might contain new features, and it ensures better protection against security threats. This feature may not work in some versions of Norton 360.

Network Proxy Settings	Lets you specify the automatic configuration details, proxy settings, and the authentication details to connect to the Internet. Programs such as LiveUpdate and Norton Insight use the specified proxy server settings to connect to the Symantec server over the Internet. LiveUpdate uses proxy settings to retrieve updates. Norton Insight uses proxy settings to obtain specific information about the files such as trust level or digital signature.

Norton Community Watch	Lets you submit selected security and application data to Symantec for analysis. Norton Community Watch protects you against new potential risks. It collects the information about new security threats from your computer and submits the information to Symantec for analysis. Symantec assesses the data to identify the new threats and resolves it. The **Detailed Error Data Collection** option is available when the **Norton Community Watch** option is turned on. **Detailed Error Data Collection** lets you allow or deny some of the detailed data submissions. These detailed data may vary depending on the Norton-specific errors and components. You can use the **Always**, **Never** and **Ask Me** options to configure the submissions.
Norton Task Notification	Lets you configure Norton 360 to show or hide the notifications that appear when Norton-specific automatic background tasks are run.

Performance Monitoring	

Lets you monitor the performance of your computer.

When the **Performance Monitoring** option is turned on, Norton 360 monitors the CPU usage and memory usage of your computer. It also records the important system activities that you performed over the period of the last three months.

In addition, Norton 360 notifies you with performance alerts when there is a high usage of your system resource by a program or process.

You have the following options when the **Performance Monitoring** option is turned on:

- **Performance Alerting**

  Lets you configure Norton 360 to detect and notify you about the increased usage of your computer resources by any program or process.

  Norton 360 alerts you with the information about the program name and the resources that the program uses. The **Details & Settings** link in the notification alert lets you view additional details about the resource consumption by the program in the **File Insight** window.

  When this option is set to **On**, Norton 360 notifies you with the performance alerts and saves the event in the Security History log. When this option is set to **Log Only**,

	Norton 360 saves the event in the Security History log but does not alert you with the notifications. You can also turn off this option if you do not want to view performance alerts. By default, this option is turned on. **Resource Threshold Profile for Alerting** Lets you configure the resource threshold profile for displaying performance alerts. When the resource consumption of a program exceeds the defined threshold limit, Norton 360 notifies you with a performance alert. You can set your threshold level to **Low**, **Medium**, or **High**. **Medium** is the default setting.

	Use Low Resource Profile On Battery Power Lets you configure Norton 360 to change the resource threshold to low profile when your computer runs on battery power. It ensures better performance of your computer on battery power. When this option is turned off, Norton 360 uses the threshold level that you set in the **Resource Threshold Profile For Alerting** option. By default, this option is turned on.

- **High-Usage Alert for:**
  - **CPU**

    When this option is turned on, Norton 360 detects and notifies you about the increased usage of the CPU resource by any program or process. By default, this option is turned on.
  - **Memory**

    When this option is turned on, Norton 360 detects and notifies you about the increased usage of memory by any program or process. By default, this option is turned on.
  - **Disk**

    When this option is turned on, Norton 360 detects and notifies you about the increased usage of your disk by any program or process. By default, this option is turned off.
  - **Handles**

    When this option is turned on, Norton 360 detects and notifies you about the increased usage of handles by any program or process. A handle is a pointer that enables a program to access or identify a resource. By default, this option is turned off.

	▪ **Program Exclusions** Lets you select specific programs to exclude from appearing in performance alerts. You can use the **Configure** option to list the programs for which you do not want to get performance alerts.
Power Saving Mode	Lets you save your battery power by suspending a list of background jobs when your computer is on battery power. By default, this option is turned on.

Product Security	Lets you secure the product and protect it from unauthorized changes. You have the following options: ▪ **Non-Admins Access to Settings** Lets you access and configure all the options in the **Settings** window from a non-admin user account as well By default, this option is turned off. You need to log in to your computer as an administrator to turn on this option. You cannot access the **Settings** window if the **Settings** window is opened in some other user account on your computer. ▪ **Norton Product Tamper Protection** Lets you protect your Norton product from an attack or modification by unknown, suspicious, or threatening applications ▪ **Settings Password Protection** Lets you protect Norton 360 settings with a password. It protects the product settings from unauthorized access ▪ **Product State Monitoring** Lets you monitor or ignore the protection status of Antivirus, Firewall, Identity Protection, and Miscellaneous features of Norton 360

Silent Mode Settings	

Lets you turn on or turn off **Silent Mode**.

You have the following options:

- **Silent Mode**

  When you turn on the **Silent Mode** option, you enable Silent Mode for a specified duration. Norton 360 suppresses all alerts and suspends the background activities for the duration that you specify.
- **Full Screen Detection**

  When you turn on the **Full Screen Detection** option, Norton 360 automatically detects the applications that you run in full-screen mode and enables Silent Mode. Norton 360 suppresses most of the alerts and suspends the background activities. The only activities that run are those that protect your computer from viruses and other security threats.
- **Quiet Mode on Detection of:**
  - **IMAPI 2.0 Disk Burn**

    When you use a Media Center application to burn a CD or DVD, Norton 360 detects the activity, and automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton 360 suppresses the background activities but continues to display alerts and notifications.
  - **Media Center TV Recording**

	When you use a Media Center application to record a TV program, Norton 360 detects the activity, and automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton 360 suppresses the background activities but continues to display alerts and notifications. ▪ **User-Specified Programs** When you run an application that is listed in the User-Specified Programs list, Norton 360 detects the activity, and automatically turns on Quiet Mode. When Quiet Mode is turned on, Norton 360 suppresses the background activities but continues to display alerts and notifications. You can configure the list of programs for which you want to turn on Quiet Mode.
Special Offer Notification	Lets you configure Norton 360 to notify you about special offers on the latest Norton products, add-ons, and other useful information from Symantec.

Automatic Resume Delay	Lets you delay the automatic running of Norton-specific background tasks when you resume your computer from hibernate mode or standby mode.
Automatic Tasks Delay	Lets you specify duration for running Norton-specific programs on your computer that run automatically when you turn on your computer. It does not delay Norton 360 protection. You can specify Automatic Tasks Delay duration for a period of 1 minute to 20 minutes. The default duration is 20 minutes.
Idle Time Out	Lets you specify the Idle Timeout duration after Norton 360 identifies your computer as idle. You can specify Idle Timeout for a period of 1 minute to 30 minutes. The default duration is 10 minutes.

Firefox Cleanup	Lets your PC run smoothly and efficiently by deleting the unused temporary files and browsing history if you use Firefox Web browser. Norton 360 automatically cleans up Internet Explorer temporary files, history, and bookmarks as a background activity. You have the following options: ▪ **Firefox Temporary File Cleanup** Lets you clean up the temporary files that get accumulated when you visit Web pages in the Firefox Web browser. ▪ **Firefox History Cleanup** Lets you clean up the history and bookmarks that get accumulated when you visit Web pages on the Firefox Web browser.

About Norton Product Tamper Protection

Norton Product Tamper Protection prevents outside programs from making changes to the Norton product. This security feature also prevents Windows System Restore from changing Norton files, which results in the **Restoration Incomplete** message.

Norton Product Tamper Protection protects Norton 360 from an attack or modification by any virus or other unknown threat. You can protect your product from accidental modification or deletion by keeping the **Norton Product Tamper Protection** option turned on.

If you want to temporarily turn off **Norton Product Tamper Protection**, you can turn it off for a specified duration.

You cannot run System Restore on your computer when **Norton Product Tamper Protection** is turned on. You must temporarily turn off **Norton Product Tamper Protection** to run a successful System Restore.

Turning off or turning on Norton Product Tamper Protection

Norton Product Tamper Protection protects the Norton 360 files from an attack or modification by any virus or other unknown threat. You can protect your product from accidental modification or deletion by keeping the **Norton Product Tamper Protection** option turned on.

If you want to temporarily turn off **Norton Product Tamper Protection**, you can turn it off for a specified duration.

You cannot run System Restore on your computer when **Norton Product Tamper Protection** is turned on. You must temporarily turn off **Norton Product Tamper Protection** to run a successful System Restore.

To turn off Norton Product Tamper Protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Product Security**, in the **Norton Product Tamper Protection** row, move the **On/Off** switch to the right to the **Off** position.
4. Click **Apply**.
5. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select how long you want to turn off Norton Product Tamper Protection.
6. Click **OK**.
7. In the **Settings** window, click **Close**.

To turn on Norton Product Tamper Protection

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Product Security**, in the **Norton Product Tamper Protection** row, move the **On/Off** switch to the left to the **On** position.
4. Click **Apply**, and then click **Close**.

About securing Norton 360 Settings using a password

You can configure Norton 360 to prevent unauthorized access to your product settings. If you share your computer with others and do not want them to modify your Norton 360 Settings, you can secure Norton 360 Settings using a password. The **Settings Password Protection** option lets you secure your Norton 360 Settings by setting up a password.

By default, **Settings Password Protection** option is turned off. You must turn on the **Settings Password Protection** option to set up a password for your product settings. You can access the **Settings Password Protection** option under **Product Security**, in the **Administrative Settings** window. The password must be between 8 and 256 characters in length.

After you set up a password for Norton 360 Settings, you must enter the password each time to access or configure your product settings. If you forget your settings password, you can reset the password in the window that appears when you choose to uninstall Norton 360. You do not need to uninstall the product to reset your password. You can use the **reset settings password** option in the **Select your Uninstall Preference** window to reset your password.

The **reset settings password** option appears in the **Select your Uninstall Preference** window only when the **Settings Password Protection** option is turned on.

You can turn off the **Settings Password Protection** option if you no longer require password protection for your Norton 360 Settings.

Securing your Norton 360 Settings using a password

You can secure your Norton 360 Settings from unauthorized access by setting up a password for your product settings. The **Settings Password Protection** option in the **Administrative Settings** window lets you secure your Norton 360 Settings using a password.

After you set up a password for Norton 360 settings you must enter the password each time to view or configure your product settings.

By default, the **Settings Password Protection** option is turned off. You must turn on the **Settings Password Protection** option to set up a password for your product settings.

The password must be between 8 and 256 characters in length.

To secure your Norton 360 Settings using a password

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. Under **Product Security**, in the **Settings Password Protection** row, move the **On/Off** switch to the left to the **On** position.
4. Do one of the following:
   - In the **Settings Password Protection** row, click **Configure**.
   - In the **Settings** window, click **Apply**.
5. In the dialog box that appears, in the **Password** box, type a password.
6. In the **Confirm Password** box, type the password again.
7. Click **OK**.
8. In the **Settings** window, click **Close**.

Turning off Norton 360 Settings password

You can protect your Norton 360 Settings with a password using the **Settings Password Protection** option. If the **Settings Password Protection** option is turned on, you need to enter the Settings password each time to view or configure your Norton 360 settings. You cannot access the product settings without providing your Settings password.

In case you forget your Settings password, you can reset it using the **reset settings password** option in the **Select Uninstall Preference** window.

You can turn off the **Settings Password Protection** option if you do not require password protection for Norton 360 settings.

To turn off Norton 360 Settings password

1. In the Norton 360 main window, click **Settings**.
2. In the **Settings** window, under **Detailed Settings**, click **Administrative Settings**.
3. In the dialog box that appears, in the **Password** box, type your Settings password, and then click **OK**.
4. In the **Settings Password Protection** row, move the **On/Off** switch to the right to the **Off** position.
5. In the **Settings** window, under **Product Security**, in the **Settings Password Protection** row, move the **On/Off** switch to the right to the **Off** position.
6. Click **Apply**, and then click **Close**.

Resetting your Norton 360 Settings password

If you forget your Norton 360 Settings password, you can reset the password. You can reset your Norton 360 Settings password using the **reset settings password** option in the **Select Uninstall Preference** window.

To access the **Select Uninstall Preference** window, you must choose to uninstall Norton 360. However, you need not uninstall the product to reset your Settings password.

The **reset settings password** option appears in the **Select Uninstall Preference** window only if the **Settings Password Protection** option is turned on. To use the **Settings Password Protection** option, go to the Norton 360 main window, and then click **Settings >General >Product Security** .

To reset your Norton 360 Settings password

1. On the Windows taskbar, click **Start** > **Control Panel**.
2. In **Windows Control Panel**, do one of the following:
   - In Windows XP, double-click **Add or Remove Programs**.
   - In Windows Vista, click **Programs and Features**.
   - In Windows 7, click **Programs** > **Programs and Features**.

     The **Programs** option in Windows 7 is available when you select the **Category** option in the **View by** drop-down list.
3. In the list of currently installed programs, do one of the following:
   - In Windows XP, click **Norton 360**, and then click **Change/Remove**.
   - In Windows Vista or Windows 7, click **Norton 360**, and then click **Uninstall/Change**.
4. At the bottom of the **Select Your Uninstall Preference** window, click **reset settings password**.
5. In the dialog box that appears, in the **Reset Password Key** box, type the randomly generated key that is displayed against **Reset Password Key**.
6. In the **New Password** box, type the new password.
7. In the **Confirm New Password** box, type the new password again.
8. Click **OK**.

Finding additional solutions

14

This chapter includes the following topics:

- Finding the version number of your product
- Finding the End-User License Agreement
- About upgrading your product
- About Norton Autofix
- Staying informed about protection issues
- About Support
- Uninstalling Norton 360

Finding the version number of your product

If you want to upgrade your Norton product or want to reach the customer support for assistance, you must know your product version number. You can find the version number of your product on your computer.

To find the version number of your product

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **About**.
   You can note the version number of your product in the window that appears.

Finding the End-User License Agreement

End-User License Agreement (EULA) is a legal document that you agree to while installing the product. EULA contains information such as the restriction on sharing or usage of the software, the user rights on the software, and the support information.

You can read the EULA to learn more about the following information:

- The usage policies of Norton 360.
- The terms and conditions for using Norton 360.

To find the End-User License Agreement

1. In Windows Explorer, double-click the drive where Norton 360 is located.
2. Double-click **Program Files > Norton 360 > MUI > *version* > 09 > 01**.
   Where *version* represents the version number of installed Norton 360.
3. Do one of the following:
   - If you are a North American user, double-click **EULA_NorthAmerica.htm**.
   - If you are an International user, double-click **EULA_ International.htm**.

About upgrading your product

Norton 360 helps you upgrade your product if you have an active subscription. You can upgrade your current product to the latest version without any cost as long as you have an active subscription with the current product. If a new version of your product is available, Norton 360 lets you download the new version.

The **Automatic Download of New Version** option automatically downloads the latest available version of Norton 360 and prompts you for free installation. To get the latest version of Norton 360, you need to

turn on the **Automatic Download of New Versio**n option. To turn on the **Automatic Download of New Version** option, go the Norton 360 main window, and then click **Settings > Administrative Settings > Automatic Download of New Version > On**.

If you choose to install the latest version of the product, Norton 360 downloads and seamlessly installs the latest version. Ensure that you have saved all your important data such as pictures and financial records before you install the new version of the product.

If you download and install the latest version of your product, your subscription status remains the same as your previous version of product. For example, you have 200 days of subscription left with your current version of product and you upgrade your product to the latest version. In this case, the subscription status of your upgraded product remains 200 days only.

If a new version is not available, the Web page informs you that no new version is available and your product is up to date. Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats.

Product upgrade is different from the program updates and the definition updates that are minor improvements to your installed product. The main differences are as follows:

- Product upgrade lets you download and install a new version of the entire product.
- Definition updates are the files that keep your Symantec products up to date with the latest antithreat technology.
- Program updates are enhancements to Norton 360 that Symantec issues periodically.

If a new version of the product is not available, ensure that you have all the latest program updates and definition updates. LiveUpdate automates the process of obtaining and installing program and definition

updates. You can use LiveUpdate to obtain the latest updates.

The upgrade process might not work if your Web browser is incompatible to communicate with the Symantec servers.

Your product must be activated and you need an Internet connection to check and install new product version.

Checking for a new version of the product

You can upgrade your product to the latest version if you have an active subscription. If you have a new version available, you can download and install the new version of your product. You can also let Norton 360 notify you when a new version of your product is available. You can do so by turning on the **Automatic Download of New Version** option in the **Administrative Settings** window. The latest version of your product may contain new and enhanced features for better protection against security threats.

When you check for a new version, details about your product such as product name and version are sent to Symantec servers. The servers then check whether a new version of the specified product is available or not.

If a new version is available, you can download and install it from the Web page. If a new version is not available, the Web page informs you about it. In such case, you can run LiveUpdate to obtain latest program and definition updates and keep the existing version of your product up to date.

The upgrade process might not work if your Web browser is incompatible to communicate with the Symantec servers. You can use Internet Explorer version 6.0 or later, Chrome version 10.0 or later, and Firefox version 3.6 or later.

Your product must be activated and you need an Internet connection to check if a new version is available and install new version of the product.

To check for a new version of the product

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **Check for New Version**.
   This option is available only if your product is activated. The Web page that appears displays whether a new version of the product is available or not.
3. Follow the on-screen instructions to download the new product.

About Norton Autofix

Norton Autofix provides additional product support with one-click access from the Norton 360 main window. Norton Autofix performs a Quick Scan of your computer and repairs problems without your intervention. If the problem persists, you can use the **Open Support Web Site** option to go to the Norton Support Web site for help using our online forum, chat, email, or telephone.

In addition, the Norton Support Web site provides access to the knowledge base articles. By using these articles, you can easily find solutions to your technical problems.

The support technicians can help you solve more complex problems by using remote-assistance technology. The remote-assistance technology allows Symantec support technicians to access your computer as remote users so that they can perform maintenance or service.

Support offerings can vary based on the language or product.

When you click the **Get Support** option in the **Support** drop-down menu, Norton 360 checks your Internet connection. To access Norton Autofix, ensure that your computer is connected to the Internet. If you use a proxy server to connect to the Internet, you must

configure the proxy settings of Norton 360. See "Configuring Network Proxy Settings" on page 51.

If you do not know your proxy settings, contact your Internet service provider or network administrator for assistance.

Solving a problem using Norton Autofix

Norton Autofix performs a Quick Scan of your computer and repairs problems without your intervention. If a problem persists, you can use the Norton Support Web site for additional online support and contact options.

Your computer must be connected to the Internet to access Norton Autofix. If you use a proxy server to connect to the Internet, you must configure the proxy settings of Norton 360.

If you do not want to proceed with the support session, you can use the **Cancel** option to bypass the scan.

To solve a problem if your computer is connected to the Internet

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. In the **Norton Autofix** window, do one of the following:
   - If the problem is not fixed automatically, click **Open Support Web Site**, and follow the on-screen instructions to find additional support.
   - If the problem is fixed, click **Close**.

To solve a problem if your computer is unable to connect to the Internet

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions in the **Checking Your Connection** window to attempt to correct your connection issue.

4. In the **Checking Your Connection** window, click **Retry**.
5. If you use a proxy server to connect to the Internet, you may be prompted to authenticate. If you are prompted, then in the **Proxy Settings Detected** window, do the following:
   - In the **Username** box, type the user name that you provided when you configured your Network Proxy settings.
   - In the **Password** box, type the password that you provided when you configured your Network Proxy settings.
   - Click **OK**.
6. If the problem still persists, in the **Norton Autofix** window, click the **click here** link.
   Under **Support Contact Numbers**, select the region, and then your country to view the contact details. You can use the contact details to contact the technical support team.

Staying informed about protection issues

If you need help using Norton 360, you can find helpful information on the Symantec Web site. It contains many useful and informative features that are especially designed to complement Norton 360, including the following:

- Detailed background information about current threats and outbreaks.
- Newsletter to which you can subscribe.
- Protection blog that lets you post your own comments and view comments from experts.

The Symantec Web site is constantly updated and enhanced, so the available resources may vary.

To stay informed about protection issues

1. Open your Web browser, and go to the following URL:
   http://www.symantec.com
2. In the **Symantec** Web site, click **Norton**.
3. In the menu bar that appears, do the following:
   - Click the **Viruses & Risks** tab, and then click any item on the left pane to find out more details about it.
   - Click the **Community** tab, and then use one of the following:

Norton Forums	Register as a user and participate in discussions. You can create your own threads of topics or take help from the existing forum discussions.
Norton Blogs	Read the messages that prominent leaders post from inside and outside Symantec and obtain information straight from the source. You can add comments or ask questions on the blogs that you are interested in.
Other Norton Communities	Check about Norton in other Web sites and social networks that are available.

About Support

If you have purchased Norton 360, you can access Support from the product.

Support offerings may vary based on the language or product.

About Norton Support Web site

The Norton Support Web site provides a full range of self-help options.

By using Norton Support Web site, you can do the following:

- Find help with your product download, product subscription, product activation, product installation, and other issues.
- Find and download the latest product manual.
- Manage your products and services using Norton Account.
- Search Norton Forum to find the additional product help about installing, configuring, and troubleshooting errors. You can also post your questions in the forum and get answers from experts. To post your questions, you need to first register for Norton Forum.
- Find information about the latest virus threats and removal tools.

Availability of support varies by region, language, or product. For additional support, go to the following URL:

http://www.norton.com/support

In addition to the self-help options, you can use the **Contact Us** option at the bottom of the Web page to

contact the technical support team in the following ways:

Live Chat	Chat in real time with a support representative. For more complex technical issues, chat offers the option to allow a support representative to connect remotely to your computer and resolve your problem.
Email	Submit your question on our Web site and receive a response by email. Email support has a slower response time than chat or phone.
Phone	Speak to a support representative in real time.
Norton Forums	Search for additional product help about installing, configuring, and troubleshooting errors.

Using the Norton Support Web site

Norton Support Web site contains answers to the most common customer questions. You can find the latest product manual, knowledge base articles, and virus removal tools.

Norton Support Web site contains problem-solving articles that are presented in an easy step-by-step format. The articles are categorized and listed on the left side of the Web page. Using the categories, you can browse through the available support topics. You can

also use the **Search Support** box to find solution using a keyword.

Norton Support Web site also contains useful links to the product manual, the Norton Account, the Norton Forum, and the spyware help under **Additional Resources**.

To use the Norton Support Web site

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions.
4. In the **Norton Autofix** window, click **Open Support Web Site**.
   The Norton Support Web page appears.
5. Follow the on-screen instructions.

About phone support

If you have a problem that you cannot resolve using Norton Autofix, use the **click here** link on the **Norton Autofix** window to get the phone number to contact a support representative.

Support offerings may vary based on the language or product.

If you cannot access phone support by using Norton Autofix, then you can access the phone support options at the following URL:

http://www.norton.com/support

Getting support by phone

When you click the **Get Support** option in the **Support** drop-down menu, Norton Autofix performs a Quick Scan of your computer and should repair your computer problems. However, if the problem persists, you can use the **Open Support Web Site** option to go to the Norton Support Web site for help by telephone, email, chat, or forum.

You can also use the **click here** link at the bottom of the **Norton Autofix** window to contact a support representative.

Availability of support varies by region. Regular telephone and Internet connection fees apply in certain countries.

To get support by phone

1. In the Norton 360 main window, click **Support**.
2. In the **Support** drop-down menu, click **Get Support**.
3. Follow the on-screen instructions.
4. At the bottom of the **Norton Autofix** window, click the **click here** link.
5. In the **Norton Autofix** window, under **Support Contact Numbers**, select the region, and then the location.
   You can use the phone number to contact a support representative.

Support policy

Symantec recommends that you have the latest version of the product, as it contains new and enhanced features for better protection against security threats. Current help and support for your Norton product can be found at the following URL:

www.norton.com/support

Symantec reserves the right to change its support policies at any time without notice. You can view the latest version of the support policy at the following URL:

www.symantec.com/supportpolicy

About keeping your subscription current

Subscription period lengths vary by Symantec product. To maintain uninterrupted protection, you must keep your subscription up to date. If you do not renew your

subscription, you cannot obtain updates of any kind and the software no longer functions.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Follow the on-screen instructions to renew your subscription.

When you renew your subscription, the definition updates and new product features are available throughout the subscription period. Please note that features may be added, modified, or removed during this period.

Worldwide service and support

Worldwide service and support solutions vary by country. To contact one of our Support offices, please go to the following Web site and select your language.

www.norton.com/support

If you are a Norton One Premium Member, go to the following Norton One support Web site for information on this topic:

https://one.norton.com/support

ClubNorton

ClubNorton is your one-stop resource center for Internet security. As a Norton customer, Symantec wants to make your experience with your computer safe, enjoyable, and productive. Whether you use your computer to manage your personal finances, shop online, or share your latest digital photos with friends and family, ClubNorton makes your experience a good one. Our goal is to consistently provide the proper tools and information to keep you up to date.

For more information, go to the following URL and select your country or region in the **Select Your Country/Region** drop-down menu:

www.clubnorton.com

The ClubNorton Web page includes a regularly updated article library, a glossary, the Norton Forums, and the Norton Update Center. You can also find the following useful links in the Web page:

- Symantec Security Check
- Subscription Troubleshooter
- Home & Home Office Security
- Product Manuals
- Product Updates
- Product Reviews
- Order Status
- Returns
- Rebates

Uninstalling Norton 360

You can remove Norton 360 from your computer in the following ways:

- From Windows **Control Panel**
- From the **Start** menu

You should print out the Uninstalling Norton 360 Help topic before continuing with the uninstallation. You cannot access online Help during uninstallation.

If you want to reinstall Norton 360 on your computer, you must uninstall Norton 360 from your computer. You can reinstall the product using the installation file that you downloaded from Symantec Web site or from the product disc. To reinstall Norton 360, follow the installation procedures that are available in the user guide.

To uninstall Norton 360 from Windows Control Panel

1 On the Windows Taskbar, click **Start > Control Panel**.

2 In Windows **Control Panel**, do one of the following:
- In Windows XP, click **Add or Remove Programs**.
- In Windows Vista, click **Programs and Features**.
- In Windows 7, click **Programs > Programs and Features**.

  The **Programs** option in Windows 7 is available when you select the **Category** option in the **View by** drop-down list.

3 In the list of currently installed programs, do one of the following:
- In Windows XP, click **Norton 360**, and then click **Change/Remove**.
- In Windows Vista or Windows 7, click **Norton 360**, and then click **Uninstall/Change**.

4 In the page that appears, under **Select Your Uninstall Preference**, click one of the following:

I plan to reinstall a Norton product. Please leave my settings behind.	Lets you retain your settings, passwords, and preferences for Norton features before you uninstall Norton 360 Select this option if you want to reinstall Norton 360 or another Norton product.
Please remove all user data.	Lets you completely remove Norton 360 without saving your settings, passwords, and preferences

5 To uninstall Norton 360, click **Next**.

6 Do one of the following:
- Click **Restart Now** (recommended) to restart your computer.
- Click **Restart Later** to restart your computer later.

Norton 360 is not fully uninstalled until you restart your computer.

To uninstall Norton 360 from the Start menu

1 On the Windows taskbar, click **Start > All Programs > Norton 360 > Uninstall Norton 360**.

2 In the page that appears, under **Select Your Uninstall Preference**, click one of the following:

I plan to reinstall a Norton product. Please leave my settings behind.	Lets you retain your settings, passwords, and preferences for Norton features before you uninstall Norton 360 Select this option if you want to reinstall Norton 360 or another Norton product.
Please remove all user data.	Lets you completely remove Norton 360 without saving your settings, passwords, and preferences

3 To uninstall Norton 360, click **Next**.

4 Do one of the following:
- Click **Restart Now** (recommended) to restart your computer.
- Click **Restart Later** to restart your computer later.

Norton 360 is not fully uninstalled until you restart your computer.

Index

A

about customer support 561
Actions window
  deleting security risks 124
  performing actions 124
  restoring security risks 124
  submission, items to Symantec 124
activation 21
  about 20
  Norton Account 24
  online backups 467
  problems 24
  troubleshooting 24
Add Rule Wizard
  opening 244
  using 245
Address Book Exclusions
  setting 286
addresses
  adding allowed 287
  adding blocked 289
  importing allowed 287
  settings 516
Administrative Settings
  about 532
Advanced Mode
  allow an event 185
adware
  found by Auto-Protect 211
adware protection settings 482
Aggressive
  SONAR Protection 185
alerts 219
  responding to 239
Allowed List 287
Antiphishing
  about 302
  hiding the toolbar 362
  showing the toolbar 362
  turning off 303
  turning on 303
AntiSpam
  about 279
  Address Book Exclusions 286
  Allowed List 287
  Blocked List 289
  Client Integration 282
  configure 515
  Feedback 291
  settings 515
  Web Query 292
antivirus settings 482
Application Ratings
  check trust level 95
  Scan Performance Profiles 97
attack signatures 260
attacks
  network 234

attention
infected files 216
infected items 158
resolve any items 158
Attention Required
about 158
resolving the risk 158
Auto-Protect
notifications 211
Automatic LiveUpdate
turning off or turning on 44
Automatic Program Control
about 239
automatic tasks 225
automatic updates 38
Autorun Restore
about 454
restoring 455

B

background jobs
about 79
monitoring 85
backup 227, 411
additional help 463
backup file categories 420
Backup Set 417
categories 103
file extensions 426
file selection 432
file types 420
Identity Safe data 350
locations 435
Norton Backup Drive 456
preparation 413
problem solving 460
restoring 447, 450
restoring selected files 451
scheduling 444
settings 471, 521
supported media 435
backup *(continued)*
turning off or turning on 469
Backup and Restore
about 350
schedules 230
backup file categories
adding or editing file extensions 427
removing file extensions 429
resetting file extensions 429
backup files
deleting 430
Backup Set
about 417
adding files and folders 432
creating 418
deleting 445
excluding files and folders 433
modifying 419
renaming 419
Backup Settings
about 521
turning off and turning on 471
backups
about 412
locations 442
online 464
online storage space 468
restore destinations 453
running 446
Bandwidth
defining usage 298
managing 296
Blocked List 289
blocking
spam 279
Boot Time Protection 204
configure 205
boot viruses 223
browser cache files 404

Browser Protection
turning on and turning off 266
Browsing
options 352
Browsing Options
about 352

C

cache files 404
Cards
about 343
adding 344
deleting 346
duplicating 346
update image 344
updating 346
categories in Norton 360
viewing details 56
CDs for backups 460
changing
scan schedules 167
cleaning up disks 401, 405
cleanups
in PC Tuneup 401
Client Integration
configuring 282
cloud technology
Cloud 168
ClubNorton
security tips 565
communication port
modifying 399
Computer
protecting 106
computers
blocking with AutoBlock 263
IP address 386
configure
Identity Safe 330
connections 106
cookies protection settings 482
CPU graph
about 73
obtaining historical data 75
resource-consuming processes 75
CPU usage
viewing 74
Creating custom scans
adding files 159
adding folders 159
custom scan
configure scan options 161
select items 160
custom scans
about 159
creating 159
deleting 163
editing 162
particular area 159
running a custom scan 162
scan frequently 159
schedule the custom scan 159
scheduling 164, 167
customer support
about 561
using 562
customizing
Allowed List 287
Blocked list 289

D

definition status 46
definition updates 39
obtaining 48
definitions
virus and spyware 45
deleting
custom scans 163
deleting custom scans
deleting 163
details links 56

detecting
security risks 210
device
adding 384
editing details 387
excluding from Intrusion Prevention scan 394
purging from exclusion list 268
remotely monitoring 376
removing from the Network Security Map 396
viewing 376
devices
changing trust level 389
Diagnostic Report
running 406
dialers protection settings 482
disk optimization 227, 402
disks
cleaning up 404
fragmentation 402
optimizing 402
domains
adding allowed 287
adding blocked 289
Download Insight
about 269
configuring alerts 275
turning off notifications 273
turning on notifications 273
Download Intelligence
turning off 272
turning on 272
DVDs for backups 460

E

email
menu 284
program 284
spam 279
error messages 219
EULA
checking 554
Events graph
monitoring activities 62

F

features
email filtering 281
Feedback
Norton AntiSpam 291
file extensions
of infected files 216
file infectors 223
files
backing up 446
fragmentation 402
scanning 227
selection, for backups 432
filter
importing allowed 287
Web Query 292
filtering
email 515
identifying email senders 287, 289
SSL 279
web-based 292
firewall
general settings 506, 509
intrusion prevention 506
program rules 506
protection settings 257, 506
removing programs 243
traffic rules 506
firewall rules
about 236
adding 244
changing the order of 255
creating 239, 245
default 237
processing order 236, 255

firewall rules *(continued)*
removing 258
turning on and off 256
Firewall settings
adding programs 241
folders
scanning 227
fragmentation 402
Full Screen Detection
about 191
Full System Scan 155
scheduling 166

G

General Rules
adding 244
removing 258

H

hack tools protection settings 482
high-risk security threats
excluding from scanning 187
home network
settings 519

I

icons in Norton 360 54
Identity Protection
categories 103
Settings 524
Identity Safe
about 313
accessing 327, 363, 368
backing up 350
changing password 358
configuring 330
information 301
logging in and out 328
logins 335
Norton toolbar 328
Identity Safe *(continued)*
password 353
restoring data 351
security 353
turning off 316
turning on 317
Identity Safe Password & Security options
about 353
Identity Safe profiles
about 317
creating 318
identity theft
Internet 301
Idle Time Optimizer
about 78
turning off 79
turning on 79
Idle Time Out
setting 231
import
logins 325
Insight Network
about 168
cloud computing 168
Insight Network scan 168
Quick Scan 168
scan 168
shortcut menu scan 168
Single File Scan 168
Insight Protection
turning off 169
turning on 169
installation
problems 36, 38
integration with email clients 282
integration with email programs 284
Internet
connection problems 106
search Explorer history 227

Internet *(continued)*
temporary files 227, 404
Intrusion AutoBlock
blocking computers permanently 265
turning on and off 263
unblocking computers 264
Intrusion Prevention 506, 511
about 260
exclusion list 266
turning individual notifications on and off 261
turning notifications on and off 261
Intrusion Prevention scan
excluding a device 394
exclusion list 266
purging devices 268
remove devices 268
IP addresses 386
finding 386
items
submitting from Quarantine 143

J

joke programs protection settings 482

L

LiveUpdate 45
about 39
Smart Definitions 42–43
technology 38
updating 226
locations for backup 435
Login
adding manually 338
changing password 341
changing URL 340
Login *(continued)*
changing user name 341
configuring 330
creating new folder 338
deleting 338
editing 338
importing 325
managing 338
saving 336
updating 343
low resource profile on battery
turning off 70
turning on 70

M

macro viruses 223
main window
messages 104
status colors 219
status messages 219
malware 221
Manage Logins
about 335
Manage Notes
about 348
Manual Repair
reviewing remaining risks in 216
Manual Repair window
reviewing remaining risks in 156
manual scan options 495
Media Center Extender
Silent Mode 195
Memory graph
about 73
obtaining historical data 75
messages 104, 219
Norton 360 219
Metered Broadband Mode
about 296

Metered Broadband Mode *(continued)*
turning off 297
turning on 297
Metered Broadband mode
defining bandwidth 298
Monthly Report
activities 101
multipartite viruses 223

N

Network
changing trust level 389
discovering devices 382
editing details 389
forming 382
joining 382
managing 375
network locations 506
Network Proxy Settings
about 48
configuring 51
Network Security Map
about 375
adding devices 384
modifying communication port 399
purging 396
removing devices 396
turning off 384
turning off Network Security Overview 381
turning on Network Security Overview 381
viewing device details 398
viewing devices 376
wireless network
viewing status 397
Network Security Overview
turning off 381
turning on 381
new version
checking 556
newsletter 565
Norton 360
about 7
about securing 549
Allowed and Blocked lists 281
background jobs 79
categories 103
details 56
EULA 554
icons 54
main window 8, 219
new version 556
password 550–551
protecting 551
registering 29
securing 550
shortcut menu 55
status 52
uninstalling 566
upgrading 554
version number 553
Norton 360 scan
about 149
command line scanning 205
Computer Scan 149
custom scans 159
Idle Time Scan 149
Insight Network 168
Insight Network scan 149
Reputation Scan 149
Norton 360 settings 257
resetting password 551
Norton Account 467
about 24
accessing 30
changing password 31
creating 29
Norton Account password 31

Norton AntiSpam 279
about 279
Address Book Exclusions 286
configure 515
Feedback 291
settings 515
SSL 279
Web Query 292
Norton Autofix
support assistants 557
Norton Backup and Restore 411
Norton Backup Drive
about 456
deleting files 459
restoring files from a Backup Set 458
Norton Bootable Recovery Tool
about 34
using 38
Norton Bootable Recovery Tool Wizard
downloading 36
Norton Community Watch
about 32
joining 32
turning off or turning on 33
Norton Firewall Diagnosis
about 259
Norton Insight
about 88
Files of Interest 92
refreshing trust level 92
trusted files 88
viewing processes 92
Norton LiveUpdate
about 39
Norton Product Tamper Protection
about 547
turning off 548
turning on 548
Norton Safe Search
searching Web 310
Norton Safe Web
about 305
turning off 310
turning on 310
Norton Tasks
about 79
Norton toolbar
about 359
accessing 363
settings 327
Notes
deleting 348
saving 348
updating 348
notification area icon 104
notifications
Auto-Protect 211
Intrusion Prevention 261

O

Office documents
embedded objects 189
scanning office documents 189
turn on or turn off 190
virus macros 189
One Click Support
using 558
online backups
activation 467
considerations 464
purchasing more storage 468
Online transactions
identity theft 313
Optimization
about 76
and performance 403
boot volume 77
running 402

optimizing 401
and fragmentation 402
Options
Client Integration 282

P

password
changing 358
editing 338
Norton Account 31
saving 336
updating 343
PC security
categories 103
PC Tuneup
categories 103
disk cleanup 405
disk optimization 402
optimization 402
Startup Manager 407
PC tuneup 401, 404
Performance
accessing 61
alerts 65
monitoring 74
performance alerts
about 65
configure 67
configure threshold 69
excluding programs 71
removing programs from exclusion list 72
turning off 67
turning off low resource profile 70
turning on 67
turning on low resource profile 70
performance improvement 402
Personal data
backing up 350
pop-up messages 219
port scans 234
problem solving 559
problem solving backups 460
problems
problems found during 216
resolve any items 216
solving 558
Product Key 22
accessing 30
product password
protecting 550
product status 46
program
patches 39
Program Control
Automatic 239
Program rules
adding 244
removing 258
program updates 39
programs
configuring Internet access 244
creating firewall rules 244
removing programs 243
programs, blocked 257
protection
dates 45
maintaining 104
quick scan 154
updates 38
protection features
monitoring 108
proxy server
configuring 51
settings 48
Pulse Updates
about 47
using 48

Q

Quarantine
adding an item 141
items, submitting for analysis 143
managing items 138
opening 138
removing items 142
restoring items 141
Quarantined Items view
adding items 111
Quick Controls
turning on or turning off 481
Quick Scan
running quick scan 154
scheduling 167
Quiet Mode
about 191, 197
disk burning 197
options 200
turning off 200
turning on 200
TV recording 197
User-Specified Programs 201

R

Real Time Exclusions
about 186
Registry Cleanup 227, 406
Remote Monitoring
setting up 382
repair
actions 216
infected files 216
removable media 216
system files 216
Reputation Scan
about 170
results 177
running Custom Scan 176
Reputation Scan *(continued)*
running Full System Scan 175
running Quick Scan 175
Responding
about 106
responding to emergencies 106
restore 411
Autorun Restore 454–455
choosing destinations 453
Identity Safe data 350
restoring backed-up files 447
selecting Backup Set 450
selecting files to restore 451
restoring items
Quarantine 141
result
resolved risks 157
Results Summary
about 157
resolved risks 157
total items scanned 157
risks
intrusions 234
malware 221
port scans 234
spyware 221
vulnerabilities 221
rules
changing 245
creating 244–245
Running custom scans
scanning required files 162
scanning required folders 162
running Full System Scan
Reputation Scan 175
running Quick Scan
Reputation Scan 175

S

Safe Surfing
about 301

Safe Web
turning off 310
turning on 310
scan at the command prompt
command line scanning 205
Scan Complete
appearing after a scan 216
Scan Complete window
appearing after a scan 156
Scan Facebook Wall
about 182
scanning 184
scanned
total items scanned 157
scanning
automatically 164
individual elements 156
problems found during 216
Scans
command line 205
Computer Scan 152
create a custom scan 159
Custom Scan 152
custom scan 227
deleting custom scans 163
file 156
floppy disk 156
folder 156
Full System Scan 152, 155
hard drive 156
Insight Network 168
manual 45
Norton Bootable Recovery Tool 38
Quick Scan 152
quick scan 154
removable drive 156
running custom scans 162
using custom 159
scheduling 228
backup and restore 230
scheduling *(continued)*
backups 444
custom scans 164
scans 164
tasks 528
scheduling custom scan
multiple schedules 164
scheduling custom scans
scheduling Full System Scan 164
searching
Security History 135
secure online storage 468
Security History
about 108
Actions window 124
adding items to the Quarantine 111
full alert history 111
importing or exporting 136
manual scan results 111
Quarantine 138
Quick Search 135
recent alert history 111
searching 135
security risks 111
submission, items to Symantec 111
suspicious email 111
viewing items 111
viewing quarantined items 111
security risks
adding to Quarantine 141
attacks 234
found by Auto-Protect 209, 211
port scans 234
removing from the Quarantine 142
restoring from Quarantine 141
security status 53
self-healing 557

Settings 475
  Administrative Settings 532
  antivirus 482
  customizing 480
  firewall 257, 506, 509
  home network 519
  Identity Protection 524
  Quick Controls 481
settings
  Task Scheduling 528
settings password
  resetting 551
  turning off 551
Settings Password Protection
  about 549
  configuring 550
  resetting 551
  turning off 551
shortcut menu 55
Signature Exclusions
  about 188
Signature Ezclusions
  excluding items 189
signatures
  including and excluding 262
Silent Mode
  about 191
  Full Screen Detection 195
  Media Center Extender 195
  turning off 193, 196
  turning on 193, 196
  turning on manually 193
Smart Definitions
  about 42
  turning on or turning off 43
Smart Firewall
  about 233
  customizing 236
SONAR Protection
  about 185
  emerging threats 185
SONAR Protection *(continued)*
  heuristic technology 185
  SONAR Advanced Mode 185
  turning off 186
  turning on 186
spyware 221, 504
  found by Auto-Protect 211
  protection settings 482
  settings 489
  system scan 155
SSL (Secure Sockets Layer)
  Norton AntiSpam 279
startup files 210
startup items
  delaying and running 409
  disabling or enabling 408
Startup Manager
  about 407
  delaying and running delayed items 409
  disabling or enabling startup items 408
status 52–53
submission, items to Symantec 143
subscription
  maintaining 564
  product updates 46
Supervisor user account
  creating firewall rules 239
Support
  AutoFix Scan 558
  Self Help 560
  solving problems 558
  worldwide service 565
Support policy 564
Symantec Security Response 143
  viewing submitted files 111
Symantec Support Web site
  about 561
  using 562

Symantec Web site
blogs and forums 559
System Insight
about 59
Events graph 59
monitoring activities 62
Performance graph 59
system status graph
activity details 64

T

Task Scheduling
settings 528
tasks
automatic 225
technical support
about 561
using 562
threats
newly discovered 46
protection from 233
Trojan horses 222
viruses 222
worms 222
trackware protection settings 482
Trojan horses 222
Trust Control
Intrusion Prevention and 260
trust level
changing 389
device 389
network 389

U

updates 38
automatically 44
manual 45
obtaining 48
Pulse Updates 47
summary 39
upgrading
new version 554
User-Specified Programs
about 201
adding programs 202
Quiet Mode 201
removing programs 203

V

version number
checking 553
virus and spyware checks
scheduling 228
virus and spyware settings 489
virus definitions 45
virus protection
system scan 155
viruses 222
boot 223
file infectors 223
macro 223
multipartite 223
protection settings 482
types 223
vulnerabilities 221
Vulnerability Protection
about 144, 146
viewing programs 145

W

Web pages
launching 340
protection 302
reporting 304
Web Query
about 292
turning off 293
turning on 293
Web sites
cache files 404

Windows temporary files 227
wireless network
    viewing status 397
worms 222

Norton from Symantec products protect consumers from traditional threats with antivirus, phishing protection, and spyware protection. They also protect against bots, drive-by downloads, and identity theft, and are light on system resources. In addition, Symantec provides services such as online backup and PC Tuneup, and is a trusted source for family online safety. For more information, please click one of the following links:

Antivirus | Phishing Protection | Spyware Protection | Online Backup